

Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

Theses and Dissertations

Student Scholarship

2018

The Sufficiency of Information Privacy Protection in Saudi Arabia

Abdulaziz Almebrad

Indiana University Maurer School of Law, aalmebra@iu.edu

Follow this and additional works at: <https://www.repository.law.indiana.edu/etd>

 Part of the [Privacy Law Commons](#)

Recommended Citation

Almebrad, Abdulaziz, "The Sufficiency of Information Privacy Protection in Saudi Arabia" (2018). *Theses and Dissertations*. 56.

<https://www.repository.law.indiana.edu/etd/56>

This Dissertation is brought to you for free and open access by the Student Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.



JEROME HALL LAW LIBRARY

INDIANA UNIVERSITY
Maurer School of Law
Bloomington

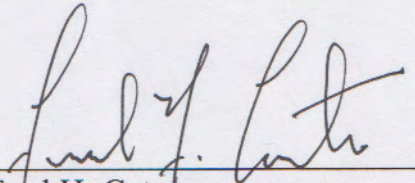
The Sufficiency of Information Privacy Protection in Saudi Arabia

Abdulaziz Almebrad

Submitted to the faculty of Indiana University Maurer School of Law,
Bloomington in partial fulfillment of the requirements for the degree: Doctor of
Juridical Science (SJD). November 2018

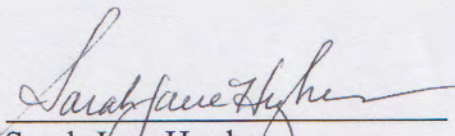
Accepted by the faculty, Indiana University, Maurer School of Law, in partial fulfillment of the requirements for the degree of Doctor of Juridical Science.

Doctoral Committee:



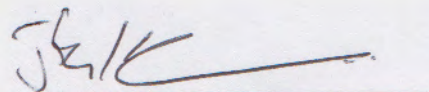
Fred H. Cate

Distinguished Professor and
C. Ben Dutton Professor of Law



Sarah Jane Hughes

University Scholar and Fellow in
Commercial Law



Jayanth Krishnan

Milt and Judi Stewart
Professor of Law

Date of the dissertation defense: November 27, 2018

DEDICATION

To My Father, Abdullah, for spending great time and effort for my education, and for being a role model as an independent thinker.

To My Mother, Jawaher, for being the perfect mother. Words cannot describe my feeling toward the greatest person in my life.

To My Lovely Wife, Afnan, for holding my hand all the way to the end of this dissertation.

To My Little Boys, Abdullah and Oday, for giving me a hug every day and saying, "good luck".

To My family's great friend, Sydney, for being a family to me and for always being there.

ACKNOWLEDGMENTS

In the first place, I would like to thank Allah for the grace he offered me in my life and for advancing me in my academic career. Second, I would like to express my greatest gratitude to my advisor Prof. Fred Cate for his valuable advice, support, and patience during my L.L.M and SJD degrees. I could receive no greater academic reward than having to write a dissertation under Prof. Fred Cate supervision. My appreciation is also extended to my dissertation committee members, Prof. Sarah Hughes and Prof. Jayanth Krishnan for sharing their insights. I would like also to express my gratitude and appreciation to the Graduate Legal Studies Office—Dean Lesley Davis, Prof. Gabrielle L. Goodwin, and Ms. May Rhea—for their generous and continuous support and advice throughout my LLM and SJD study at the Maurer School of Law on both the personal and the professional level. Lastly, but most importantly, my deep appreciation to my parents for their endless support throughout my life. My very special thanks go to my wife, Afnan, for being supportive and patient throughout my study.

ABSTRACT

Since the technology revolution, the rules of privacy law have rapidly changed in many countries to keep pace with new privacy challenges. Surprisingly, Saudi Arabia has no specific data protection legislation. This does not necessarily mean that people's personal information is totally unprotected. In fact, the legal system in Saudi Arabia relies on both Islamic jurisprudence and written laws. Sharia law, the paramount body of law in Saudi Arabia, places a high value on an individual's privacy and prohibits any invasions therein, except in very limited circumstances. Moreover, other provisions relating to the sanctity and safety of individuals' personal data are spread out over several legislative instruments. The dissertation discusses whether the current level of protection of individuals' rights to privacy—particularly in the digital world— offered by both Sharia law and Saudi regulations is sufficient and effective; and recommends practical steps that can be taken to develop a stronger information privacy system.

TABLE of CONTENT:

<u>Dedication</u>	ii
<u>Acknowledgement</u>	iii
<u>Abstract</u>	iv
<u>Introduction</u>	1
<u>Chapter one: Privacy in Sharia law</u>	
❖ <u>Introduction</u>	6
❖ <u>Background</u>	9
➤ <u>Sources of Sharia Law</u>	9
▪ The Quran	9
▪ The Sunnah	10
▪ Scholars' consensus (<i>ijma</i>)	11
▪ Reasoning by analogy (<i>qiyas</i>)	12
➤ <u>The School of Law</u>	13
❖ <u>The primary Islamic principles protecting information privacy</u>	13
➤ <u>The prohibition of spying</u>	14
▪ The general prohibition of spying in Islam	14
▪ Spying at someone's home	15
▪ The usage of technology to invade someone's house	16
▪ Private correspondence	20
▪ Personal letters	21
▪ Spying on public places	22
• Spying on public places by looking	23
• Listening to private conversations in public places	24
➤ <u>Seeking Permission</u>	26
▪ Seeking permission before entering someone's home	27
• What is "home"?	27
▪ The role of General Custom	28
▪ The purpose of seeking permission	29
▪ Seeking permission is required	30
• General permission	30
• Special permission/aggravating circumstances	30
▪ How to seek permission	33
• Explicit permission	33
• Implied permission	35
▪ The scope of the permission	36
▪ The authority to give permission	37
➤ <u>Information pertaining to others</u>	38
▪ Concealing others' damaging information (<i>sater al-awrat</i>)	39
▪ Keeping others' confidential information (<i>kitman alsir</i>)	43
• Professional relationships	45
• Non-professional relationships	46
❖ <u>Penalties/ punishment</u>	48
➤ <u>Material harm</u>	49
➤ <u>Moral harm</u>	50

❖ Conclusion	52
Chapter 2: Information Privacy in Saudi Laws	
❖ Introduction	54
➤ The Legal System in Saudi Arabia	54
▪ Introduction to the Basic Law of Saudi Arabia	54
▪ State Authorities	55
• Executive Branch	55
• The Legislative (Regulatory) Branch	56
• The Judicial Branch	58
♦ Sharia Courts	58
♦ The Board of Grievances	60
❖ Privacy in Saudi Arabia’s Legislation	60
➤ The Basic Law of Governance of 1992	61
➤ Law of Criminal Procedures (2013)	62
➤ The Anti-Cyber Crime Law (2007)	64
➤ E-Transaction Law and its Executive Regulation	74
➤ The Telecommunications Law and its Executive Regulation	79
➤ Cloud Computing Regulatory Framework (2018)	86
➤ Banking Consumer Protection Principles (2013)	90
➤ The Law of Practicing Healthcare Professions and its Implementing Regulations ...93	
➤ The Draft Law of E-Commerce 2014	94
➤ Civil Affairs Law 1986	98
❖ Conclusion	98
Chapter 3: Why is Saudi Arabia’s current level of protection regarding individuals’ private information deficient and thus ineffective?	
❖ Introduction	101
❖ The primary obstacles affecting the insufficiency of the current level of information privacy protection in Saudi Arabia	102
➤ Obstacle 1: The absence of a comprehensive data protection law	102
➤ Obstacle 2: The Saudi courts’ decisions on compensation for moral damages are inconsistent	106
➤ Obstacle 3: Sharia Principles are too broad to address privacy concerns in the digital world, and most of the Saudi judges are not qualified as a mujtahid	110
➤ Obstacle 4: The judiciary system in Saudi Arabia does not recognize class action lawsuits	119
➤ Obstacle 5: The courts’ decisions are not regularly published such that the public can access them, and the decision of one court is not usually binding in other courts	121
➤ Obstacle 6: Saudi citizens are not fully aware of their privacy rights	123
➤ Obstacle 7: The level of legal qualification for information privacy is weak	129
❖ Conclusion	131
Chapter 4: The future of information privacy in Saudi Arabia	
❖ Introduction	133
A- Why does Saudi Arabia need to improve on its information privacy protections?	
1- To meet the level of protection granted via Sharia law in an era characterized by technological advances	134

2- Technology plays a vital role in the future of Saudi Arabia	135
a. Developing a digital infrastructure.....	135
b. Leader in E-government.....	136
c. Building “Smart Cities”	137
d. E-commerce in the retail sector.....	138
e. Investing in emerging technologies	138
B- <u>Recommendations for protecting information privacy in Saudi Arabia</u>	
1- Adopting a formal law.....	142
a. Comprehensive law	143
b. Sectoral laws.....	144
c. Other forms of formal laws.....	145
➤ Adopting a comprehensive data protection (GDPR-like) law is the best long-term goal for Saudi Arabia	145
▪ The advantages of adopting a comprehensive data protection law in Saudi Arabia.....	146
▪ The challenges of adopting a comprehensive data protection law in Saudi Arabia.....	148
• The high cost for both the government and the private sector.....	148
• The lack of technicians specialized in information security and privacy professionals.....	149
• Unsophisticated judicial regimes.....	151
2- Adopting the co-regulatory approach as an intermediate step toward a comprehensive model.....	152
3- Establishing an oversight authority.....	155
4- Judicial reforms.....	157
a. Establishing a judicial data protection committee.....	157
b. Allowing class-action cases.....	158
c. Compensating moral harm.....	158
5- Raising the level of privacy education.....	159
<u>Conclusion</u>	162

Introduction

The technological revolution brought with it new challenges related to privacy, and this in turn prompted many countries to keep pace via rapidly changing privacy laws. In Saudi Arabia, technology plays a crucial role in the country's present-day and future, as 60% of the country's population is under the age of 29,¹ 94% of people in Saudi Arabia use the Internet,² and the number of e-commerce transactions that have been completed have increased dramatically in recent years. As a part of Saudi Arabia's long-term plan to diversify its economy, the government plans to invest in and utilize technology in a number of ways, such as building smart cities, improving e-government services, and enhancing e-commerce. Thus, it has become much easier to access individuals' personal information, and this poses an unprecedented risk to individual privacy.³

Surprisingly, Saudi Arabia has no specific data protection legislation. This does not necessarily mean that people's personal information is entirely unprotected. In fact, the legal system in Saudi Arabia relies on both Islamic jurisprudence and written laws. Sharia law, the paramount body of law in Saudi Arabia, places a high value on an individual's privacy and prohibits any invasions therein, except in very limited circumstances. Moreover, other provisions relating to the sanctity and safety of individuals' personal data are spread out over several legislative instruments. The question is whether the current level of protection of individuals' rights to privacy—particularly in the digital world—offered by both Sharia law and Saudi

¹ KINGDOM OF SAUDI ARABIA GENERAL AUTHORITY FOR STATISTICS, POPULATION BY GENDER, AGE GROUPS AND NATIONALITY (SAUDI/NON-SAUDI) (2018) *available at* <https://www.stats.gov.sa/en/43>.

² COMMUNICATIONS AND INFORMATION TECHNOLOGY COMMISSION, INTERNET USAGE IN SAUDI ARABIA (2016), *available at* http://www.citc.gov.sa/ar/reportsandstudies/studies/Documents/PublicIndividualReport2016V5_Ar.pdf.

³ In 2016, 1,000 cyber security attacks targeting critical infrastructure, seeking to steal data, and causing service interruptions. *See* MELISSA HATHAWAY, FRANCESCA SPIDALIERI & FAHAD ALSOWAILM, KINGDOM OF SAUDI ARABIA CYBER READINESS AT A GLANCE (2017), *available at* <https://www.belfercenter.org/sites/default/files/files/publication/cr-2.0-ksa.pdf>.

regulations is sufficient and effective; and if it isn't, then it is necessary to determine what steps can be taken to develop a stronger information privacy system.

During the classical Islamic period,⁴ the word "privacy," as it is defined today, did not exist, so the applications and the rules that value individual privacy can be found in many different areas such as theft, seeking permission, trust, exposing others' secrets, and general morals.⁵ During the last century, a few scholars tried to gather the texts related to individual privacy from the Quran and Sunnah, as well as from jurists' opinions, and label them under a single heading: "Privacy in Islam." These attempts, however, resulted primarily from the scholars collecting texts from the Quran and Sunnah and addressing privacy in Islam generally without distinguishing between the moral and legal rules. The collection of these texts represents a significant step. However, since these texts are roughly 1,400 years old, it is critical to be able to draw rules and principles from them that could be applied to more contemporary privacy issues and contexts, most of which stem from the use of technology. Thus, this dissertation highlights the key principles and rules that govern individuals' information privacy (i.e., the general prohibition of spying, the command to seek permission, and the command to keep others' secrets) and examines, in particular, how sufficiently these principles address privacy issues in the modern age.

On the other hand, although Saudi Arabia does not have a comprehensive data protection law, it has several laws and regulations that offer some protection to individuals regarding their personal information. Most of these regulations do not place information privacy among their

⁴ By "classical," I refer to the period from the rise of Islam through the thirteenth century.

⁵ ABD AL-LATIF ALHAMIM, EHTRAM AL-HAYAT ALKASAH FI ISLAM [RESPECT FOR PRIVATE LIFE IN ISLAM] 98-101 (2003).

main objectives. Therefore, each one of these regulations offers individuals limited protection of their private information and uses broad language when discussing matters related to privacy.

Studies that review all laws that somehow protect individuals' private information in Saudi Arabia are rare. The published legal studies in the field of privacy law in Saudi Arabia discuss primarily the protection of privacy provided by a particular law⁶ or one aspect of privacy such as compensation associated with one's privacy being violated or violating privacy through espionage.⁷ Thus, the description of the legal protection provided via both Sharia principles and Saudi regulation is a critical part of this dissertation because it is the first step in assessing the sufficiency and efficiency of these legal provisions and principles. This dissertation goes beyond merely describing the legal provisions, as it also points out the primary issues or variables that affect the current level of protection. The obstacles include a legislative vacuum, an inefficient judicial system, and a relative lack of awareness among society.

This dissertation will be beneficial not only to Saudi Arabia, but it will also benefit other developing countries in the region that share several traits with Saudi Arabia such as culture, economy, and, most importantly, Sharia law. By building a new consistent information privacy system, many international corporations will be encouraged to enter Saudi markets, as their

⁶ See Mansour Alsolami, Almasoliah Almadaniah Lentihak Alkusosyah fi Ndam Aljaraem Almalomatiah fi Alsaudiah [Civil Liability for Violating Person's Privacy under The Anti-Cyber Crime Law of 2007 in Saudi Arabia] (2010) (unpublished thesis, Naif Arab University for Security Sciences) (on file with Naif Arab University for Security Sciences Library).

⁷ See Mohammad Al-Qahtani, Hemayat Alkusosyah Lmustakdmin Mwaq Altawasel Alejtmaeyah [Privacy Protection for Users of Social Networking Sites] (2015) (unpublished thesis, Naif Arab University for Security Sciences) (on file with Naif Arab University for Security Sciences Library); MSFER AL-QAHTANI, ALHYMAYAH ALMADANIYH L ALMAELOMAT ALSHAKSYAH [CIVIL PROTECTION OF PERSONAL COMPUTER INFORMATION: COMPENSATION IN ISLAMIC JURISPRUDENCE AND THE LEGISLATION IN SAUDI ARABIA] (2005). See Also Suria Alshahri, Almasolyah Alagnaeyah l Altajasys Alelectroni fi Alandmah Alsudiah [Criminal Responsibility for Electric Espionage in Saudi Regulations] (2015) (unpublished thesis, Naif Arab University for Security Sciences) (on file with Naif Arab University for Security Sciences Library).

investment risks will be reduced thanks to a clear and consistent information privacy system. More importantly, individuals in Saudi Arabia will receive the high level of protection promised via Sharia law.

Since this is a new topic in Saudi Arabia, few books and articles have been written on the issue of data protection in Saudi Arabia mostly in Arabic. Further, the courts' decisions are not regularly collected and made available to the public, and there are no precedents that are binding to other courts under Saudi Arabia's legal system. As such, this study relies on newspaper articles, investigative news reporting, and key books that explain Sharia law, which, in Saudi Arabia, are derived primarily from Hanbali School.

➤ **Research roadmap**

The dissertation is divided into four main chapters. The first chapter starts with a brief explanation of the importance of studying the right to privacy under Sharia law. It also provides background on Sharia law and its sources. The chapter serves primarily to analyze texts from the Quran and Sunnah and various Sharia scholars' opinions. In doing this, the chapter examines these texts in accordance with three main principles: the prohibition of spying, the obligation of asking permission, and concealing information pertaining to others. Lastly, the chapter discusses the punishment associated with violating these principles under Sharia law.

The second chapter demonstrates the right to privacy, especially as it pertains to personal information protection, under the Saudi legal system. Many provisions relating to the sanctity and safety of individuals' personal data are spread out over a number of legislative instruments. The chapter begins by providing background on the Saudi legal system. The primary purpose of the chapter is to provide an analysis of each law and regulation and to examine the clarity and sufficiency of the current Saudi information privacy system. These laws include the Anti-cyber

Crimes Law, the E-Transaction Law, the Telecommunications Law and its Executive Regulation, the Law of Practicing Healthcare Professions and its Executive Regulations, the Banking Consumer Protection Principles, and the Cloud Computing Regulatory Framework.

The third chapter notes the primary obstacles that serve to weaken the level of information privacy protection in Saudi Arabia. The chapter addresses the primary reasons why the current level of protection provided to individuals regarding their personal information is lacking. Among these reasons are a legislative vacuum, an inefficient judicial system, and a relative lack of awareness among society.

The fourth chapter discusses the reasons why the government of Saudi Arabia should act to improve the level of information privacy protection it offers its citizens. It also explains the importance of technology to the future of Saudi Arabia as a country. That is, without a strong information privacy system, the Saudi's plan to develop the technology market might be jeopardized. Next, the chapter describes different approaches that countries around the world use to protect individuals' data, explains the advantages and disadvantages of each model, and discusses the model that might best apply to Saudi Arabia in its attempts to improve the level of data protection it offers its citizens without negatively affecting the market. Since the adoption of a strict data protection law might negatively impact the Saudi market, the recommendations focus on building a solid foundation before adopting a strict data protection law, which might take several years. The recommendations also discuss which approach would best serve Saudi Arabia in the coming years as it works to a stronger foundation.

Chapter 1: Privacy in Sharia Law

❖ Introduction

Islam began in the Arabian Peninsula in the 7th century, and it spread around the world to reach more than 1.6 billion Muslims living in many different countries. Today, Islam is the official religion of roughly 46 countries, Sharia law is the only source of law in five countries and the main source of law in four other countries, and Sharia is one of the primary sources of law in six other countries.⁸

By issuing strict rules aimed at protecting an individual's privacy, Islam effectively changed the Arab community. For example, during the pre-Islam period, Arabs freely visited others' homes without first obtaining permission. This was inconvenient to the homeowners or residents, especially women, who might have removed their clothing in order to keep cool in the hot climate.⁹ As such, to protect residents' privacy, the Quran implemented new rules that restrict the times during which people are permitted visit others' homes and make clear how one should go about properly seeking permission before entering others' houses.¹⁰ These rules are not merely about the sanctity of the home; they address other private matters as well, including personal correspondence, private conversation, and personal financial affairs.¹¹ In addition, in some circumstances, the privacy rules serve to regulate the relationships among family members who dwell within the same household to ensure that individuals' personal information is protected from any kind of invasion.

⁸ Muhammad Mufti, *aldowal alati tans dasaretha ala Islam [States Whose Constitutions Stipulates Islam]* 2012, <http://www.alukah.net/culture/0/40294/>.

⁹ HUSNI AL-JUNDI, DAMANAT HURMAT AL-HAYAT AL-KHASSAH 59 (1993).

¹⁰ In Quran, "O you who believe! Do not enter houses other than your own houses until you have asked permission and saluted their inmates; this is better for you, that you may be mindful." Al-noor 27. Exegesis indicate that this verse was revealed after a complaint was raised by a Muslim woman to the Prophet "PBUH" regarding the issue of men from her relatives entering her house without permission while she is wearing inappropriate clothes. *Id.*

¹¹ MOHAMMAD HASHIM KAMALI, THE DIGNITY OF MAN: AN ISLAMIC PERSPECTIVE 61 (2002).

It might be worth considering why one would even bother to examine Islamic history in order to search for principles that might solve today's issues when today most Islamic countries are bound by international covenants¹² and have constitutions and laws that establish the right to privacy as a fundamental human right, require warrants to enter homes, and limit intrusions with regard to private communications and correspondence. There are three major reasons why looking into Islamic history is worthwhile.

First, building a new law based on the rules associated with classic Islamic sources will increase compliance with the law because Muslims take into account the Islamic pedigree of a law when determining that law's legitimacy.¹³ Further, the concept of Islamic law is more comprehensive than the modern legal system.¹⁴ In particular, the modern legal system places the state in charge of either authorizing or forbidding certain actions; the state is also tasked with punishing those who violate its laws. The state is not interested in what people do outside of its spheres of influence or concern. On the other hand, Islamic law has a wide-ranging interest in human acts. It categorizes them into various types, ranging from the moral to the legal, but it does not consciously differentiate what is moral and what is legal. Thus, under Islamic law, all acts are regarded and categorized according to five norms: prohibited, obligatory, recommended, disapproved, and neutral.

¹² The 1966 International Covenant on Civil and Political Rights and the 1984 Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment. Muslim-majority countries have themselves adopted "Islamic" declarations of human rights, specifically a 1981 Universal Islamic Declaration of Human Rights, a 1990 Cairo Declaration on Human Rights in Islam, and a 1994 Arab Charter on Human Rights.

¹³ Sadiq Reza, *Islam's Fourth Amendment: Search and Seizure in Islamic Doctrine and Muslim Practice*, 40 *Geo. J. Int'l L.* 703, 704-5 (2009)

¹⁴ *Id.*

Committing a forbidden action, such as breaching a contract or spying on another's home, will result in punishment for the wrongdoer.¹⁵ One will also receive punishment for failing to perform an obligatory action, such as praying and seeking permission before entering others' homes.¹⁶ Both of these categories involve punishment upon non-compliance. Carrying out a disapproved act, however, such as standing in front of the door when asking permission, entails no punishment.¹⁷ Similarly, not performing a recommended act (Sunnah), such as helping the poor, will not result punishment. However, if a person is compliant and thus performs a recommended act or refrains from carrying out a disapproved act, then he or she will be rewarded, although the reward might come in the Hereafter.¹⁸ Finally, neutral acts, which are neither prescribed nor recommended, result in neither reward nor punishment.

Second, Sharia law has superiority over any other written law in many Islamic countries such as Saudi Arabia, the focus of the dissertation. In other words, all laws enacted in Saudi Arabia must comply with Sharia law.¹⁹ Further, in the absence of written law, judges in Saudi Arabia will rely on the Islamic jurisprudence when making decisions. As such, any research that traces the principles aimed at protecting individuals' privacy from Islamic sources and connects these principles with today's issues will help judges to take affirmative actions to guarantee the protection of individuals' personal information.²⁰

¹⁵ WAEL B. HALLAQ, AN INTRODUCTION TO ISLAMIC LAW 19 (2009).

¹⁶ I will explain the requirement of seeking permission before entering the house in this chapter later.

¹⁷ Sunan Abi Dawud 5186, Book 43, Hadith 414 "When the Messenger of Allah (PBU) came to some people's door, he did not face it squarely, but faced the right or left corner, and said: Peace be upon you! Peace be upon you! That was because there were no curtains on the doors of the house at that time". Al-Qurtbi in his book of Quran exegesis explains, "If he found the door closed, he can stand wherever he likes". 19 AL-QURTBI, TAFSIR AL-QURTUBI 200 (Dar Alkutb, 2ed ed. 1064).

¹⁸ Hallaq, *Supra* note 15.

¹⁹ "The Kingdom of Saudi Arabia is a fully sovereign Arab Islamic State. Its religion shall be Islam and its constitution shall be the Book of God and the Sunnah (Traditions) of His Messenger, may God's blessings and peace be upon him (PBUH)." The Basic Law of Governance, SA §1. (1992).

²⁰ The Basic Law of Governance, SA §1. (1992).

Third, for academic reasons, it is important to examine the existence and the scope of Islamic principles or rules that protect individuals' privacy and compare these principles to those associated with modern laws.

This chapter is divided into three sections. The first section provides background regarding Sharia law and its sources as well as schools of Islamic jurisprudence. The second section, which is the main section of this chapter, discusses the primary Islamic principles that regulate the individual's personal information. This section does not seek to examine all aspects of privacy in Islam. Instead, the section concentrates on the key principles that serve to regulate personal privacy under Sharia law; this allows the author to evaluate the level of protection granted to the people under Sharia. The principles discussed include the prohibition of spying, the obligation of asking permission, and concealing information pertaining to others. The third section discusses punishment under Sharia, particularly punishment that results when an individual violates another's privacy.

❖ Background

➤ Sources of Sharia law

▪ The Quran²¹

The Quran, which is the actual word of God (Allah) as revealed to the Prophet (PBUH) by the angel Gabriel, is the most sacred source of law in Islam.²² The Quran, which was

²¹ There are other names used to refer to the Quran, which are mentioned in different Verses of the Quran. For example, the book "Al-Kitab", the discernment or distinction "Al-Furqan", and a reminder "Al-Thaker" all are synonyms of the Quran. See R. BHALA, UNDERSTANDING ISLAMIC LAW: SHARIA 292 (2011).

²² *Id.*

completed before the death of the Prophet (PBUH),²³ has only one version that is written in Arabic, and this version continues to be utilized today.²⁴ None of the words or letters contained within the Quran can be altered.²⁵ In the Quran, God presents knowledge about human beliefs, about God himself, and about how the believer should conduct himself in this world.²⁶ This human conduct is the domain of law.²⁷ For instance, in the Quran, there are laws that deal with crime, marriage, civility, and borrowing.²⁸

▪ The Sunnah

The Sunnah is the second primary source of Sharia law. It is comprised of the traditions of the Prophet (PBUH), which consist of deeds, utterances and silent approval.²⁹ The importance of the Sunnah, as the second source, was ordained in several verses in the Quran.³⁰ It came to

²³ In 633, the Quran was written during the life of the prophet, but it was compiled of 114 chapters and 6,236 verses, after the death of the Prophet “PBUH”. See Etim E. Okon, *The Sources and Schools Of Islamic Jurisprudence*, 3 AM. J. SOC. MGMT. SCI. 106, 106-111 (2012).

²⁴ C. G. WEERAMANTRY, *ISLAMIC JURISPRUDENCE: AN INTERNATIONAL PERSPECTIVE* 7 (1988).

²⁵ *Id.*

²⁶ Hallaq, *Supra* note 15, at 16.

²⁷ MOHAMMAD HASHIM KAMALI, *PRINCIPLES OF ISLAMIC JURISPRUDENCE* 25 (2005). Kamali notices that Quran has around 350 verses that contain regulations and laws for both acts of worship and civic life. The 350 verses are divided into four types of regulations. Religious regulations, account for 140 of the 350 verses and are the most prevalent of the four. Religious regulations include subjects like prayer, fasting, Zakat, and pilgrimage or Hajj. Each of the remaining three types is made up of about verses each. Personal matters cover marriage, divorce, child custody, and inheritance. Commercial regulations refer to subjects such as sales, loan, contracts, and security transactions. The fourth type of regulation deals with justice, evidence, witnesses, and consultation. These are portions of the Islamic primary principles that all other laws and regulations must be built on them.

²⁸ Weeramantry, *Supra* note 24, at 5.

²⁹ The literal meaning of Sunnah in Arabic is a manner of acting, a rule of conduct, a mode of life. See Okon, *Supra* note 23.

³⁰ In the Quran, the Sunnah is mentioned 16 times. For example, “Whatsoever the Messenger give you, take it and whatsoever he forbids, abstain” (Quran, Surah Al-nor, verse (24:54). Ali Ahmari-Moghaddam, *Towards International Islamic Human Rights: A Comparative Study of Islamic Law, Shari’ah, with Universal Human Rights as Defined in the International Bill of Human Rights* (2012) (unpublished LL.M thesis, University of Toronto), available at https://tspace.library.utoronto.ca/bitstream/1807/32513/5/AhmariMoghaddam_Ali_20126_LLM_thesis.pdf.

clarify some of the verses in Quran and fill the gaps in the laws where the Quran is silent.³¹ The Sunnah, or the way of the Prophet (PBUH), is also called the Hadith.³²

There was no attempt to collect or record the Sunnah during the life of the Prophet.³³ After the death of the Prophet and the completion of the Quran, however, the Islamic scholars worked tirelessly to collect the hadiths and check their accuracy. Thus, they established the science of *isnad* (“chain of transmission”). In order for a hadith to be considered authentic, it has to be connected back to the Prophet (PBUH) in a reliable manner. Every hadith has been graded as correct, good, weak, or false. The gradations depend on the number of individuals who transmit the hadith, their reputations for “accuracy and honesty, and the degree of consistency in the wording of the hadith in different transmissions.”³⁴ The author of this dissertation does not rely on or use as evidence any weak or false hadiths.

- **Scholars’ consensus (*ijma*)**

Scholars’ consensus (*ijma*) serves as the third source of Sharia law and the first of the four dependent sources.³⁵ If the primary sources, the Quran and Sunnah, do not directly address a question, one can turn to the general consensus among Islamic scholars of a particular age in relation to the legal rule to find the answer.³⁶ If all of the Islamic scholars agree on a given decision, it becomes binding legal rule and part of the permanent body of Islamic

³¹ The Quran and Sunnah must be harmonized. In a case of contradiction, the Quran prevails. *See* Weeramantry, *supra* note 24, at 34.

³² The terms “Sunnah” and “Hadith” overlap in most of the places and are separate in other places. There is a slight difference in meaning between these words. *See generally* Bhala, *supra* note 21, at 273.

³³ Some scholars believe the possibility of confusion between Quran and Sunnah was the reason behind not recording the Sunnah during the life of the prophet. In fact, there is a Hadith that the Prophet "PBUH" said, "Do not take down anything from me, and he who took down anything from me except the Qur'an, he should efface that" (Sahih Muslim 3004, Book 55, Hadith 92). *See* Weeramantry, *supra* note 24, at 35.

³⁴ Bhala, *supra* note 21, at 278.

³⁵ Weeramantry, *supra* note 24, at 39.

³⁶ *Id.*

jurisprudence.³⁷ The authority of ijma is rooted in the practices of honoring the unanimous decision and distrusting individual opinion.³⁸ In fact, the Prophet (PBUH) himself endorses the ijma as he indicated when he said, “My nation will not unite through misguidance, so if you see them differing, follow the great majority.”³⁹ The agreement among Islamic scholars during a particular age must be unanimous if it is to be considered ijma.⁴⁰ In other words, a majority opinion will not result in a binding decision; only absolute consensus will yield this. Today, a clear consensus might take years to achieve because of the distance between Muslim countries and the number of Muslim scholars.⁴¹

▪ **Reasoning by analogy (*qiyas*)**

If all three sources above fail to provide a legal answer to address a new issue, the Islamic scholars must make analogical comparison between a current rule from the Quran or Sunnah and the new issue that possesses a similar set of facts.⁴² This sort of analogy is called a qiyas.⁴³ Unlike ijma, where the scholars create a new law, qiyas is a useful tool to interpret existing law and extend its application to a new issue.⁴⁴ Qiyas is the fourth and last unanimously accepted source of law in Islamic jurisprudence. All Sunni schools recognize qiyas as a valid source of law with some disagreement about how often they should use the qiyas as source.⁴⁵ Today, qiyas is considered a valuable tool that permits scholars to address issues that are a part of modern life

³⁷ *Id.*

³⁸ *Id.*

³⁹ Sunan Ibn Majah 3950, Book 36, Hadith 25.

⁴⁰ Ijma might be established actively by stated consensus or action, or passively by failing to object and remaining silent. Bhala, *supra* note 21, at 286.

⁴¹ *Id.* at 287

⁴² *Id.* at 288

⁴³ The literal meaning of Qiyas in Arabic is “measurement.” *Id.*

⁴⁴ *Id.* at 289

⁴⁵ *Id.* at 290.

such as technology. Since dissertation focuses on new issues pertinent to individuals' personal information, qiyas will serve as the most practical means of addressing these matters.

➤ **The schools of law**

There are four major schools of Islamic Sunni jurisprudence: the Hanafi School, the Maliki School, the Shafi'i School, and the Hanbali School. These schools were developed during the second and third centuries of Islam. For Muslims, it is not obligatory to follow only one school; rather, a different school may be applied to each decision in a person's life.⁴⁶ All of these schools are recognized and well respected within the Muslim world. However, historically, some nations prefer one school to another. In Saudi Arabia, for example, Hanbali is the preferred school, but a judge is not bound by any law to adhere to this school. If a judge, in any case, happened to believe that another school was more applicable and yielded a more appropriate ruling, then he may choose to follow that school.⁴⁷ In this dissertation, the discussion draws on jurists from different schools. The aim of this chapter is to shape the privacy theory under Islamic law without adhering to one particular school.

❖ **The primary Islamic principles protecting information privacy**

While the word "privacy" (*kososiah*), as it is defined today, did not exist during the classical Islamic period,⁴⁸ the applications and the rules that value individual privacy can be found in many areas such as theft, seeking permission, trust, exposing others' secrets, and general morals.⁴⁹ Today, technology has brought about new privacy challenges that need to be addressed via Islamic principles. The primary goal of this chapter is not to cover how Islam protects an

⁴⁶ Weeramantry, *supra* note 24, at 49.

⁴⁷ For more information about the Islamic schools and the similarities and differences between each school. See MOHAMMED ABU ZAHRA, HISTORY OF ISLAMIC SCHOOLS 359 (Dar al-Fiqr al-Arabi 1946)

⁴⁸ By "classical" I refer to the period from the rise of Islam through the thirteen-century.

⁴⁹ Alhamim, *supra* note 5 at 98.

individual's privacy in every matter, but to highlight the main principles and rules that govern the individual's information privacy and examine, in particular, how sufficiently these principles address privacy issues in the modern age.

After collecting and analyzing most of the texts from the Quran and Sunnah, as well as from Islamic jurists, that have to do with protecting the right to privacy, it became increasingly clear to the author of this dissertation that Sharia protects the right to privacy primarily via three principles: the general prohibition of spying, the command to seek permission, and the command to keep others' secrets.

➤ **The prohibition of spying**

▪ **The general prohibition of spying in Islam**

Many verses of the Holy Quran and Sunnah explicitly prohibit any kind of spying or espionage (*al-tagassas*) in general. Other provisions deriving from Sunnah and from the practice and understanding of the Companions of the Prophet specifically describe what constitutes a forbidden act of espionage and the level of prohibition based on various factors. The most general and directed verses from the Quran and Sunnah are as follows: "O you who have believed, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other."⁵⁰

From the Sunnah, The Prophet (PBUH) said, "Do not harm the Muslims, nor revile them, nor spy on them to expose their secrets. For indeed whoever tries to expose his Muslims brother's secrets, Allah exposes his secrets wide open, even if he were in the depth of his house."⁵¹

⁵⁰ Quran, Alhujrat, (49:12).

⁵¹ Jami` at-Tirmidhi 2032, Book 27, Hadith 138.

In this verse from Quran and the report from the Sunnah, spying is clearly forbidden for all Muslims, individuals and state actors alike.⁵² Muslim scholars tried to define the meaning of al-tagassas as the act of spying or espionage. Al-Ghazali describes al-tagassas, in general, as the search for something in order to know what is otherwise not known and not permitted by the Sharia.⁵³ Al Jundi explained further that al-tagassas is the action of searching for information about a person, which is believed to be private or confidential, by looking, listening, or searching through the person's papers without seeking prior permission.⁵⁴

The rules of al-tagassas in Islam and the level of seriousness associated with violating these rules vary according to several factors such as the place, the time, the custom of the people. For example, looking in someone's house without permission might result in allowing the resident to poke out the peeper's eye without being held liable for the peeper's loss of sight.⁵⁵ In contrast, listening to two people hold a private but loud conversation in a public place is not a punishable crime; rather, the listener in this case would only be performing a disapproved action.

▪ Spying at someone's home

Sharia law in both the Quran and Sunnah grants the highest level of privacy and thus protection to individuals' homes against any kind invasion. Since classic Islamic scholars did not recognize "privacy" as a right by itself, it is vital to ask why Islam gives homes special protection. Is it to protect the property, the safety of the resident, or the privacy of the residents?

⁵² A. E. MAYER, ISLAM AND HUMAN RIGHTS: TRADITION AND POLITICS 723 (2013).

⁵³ Ida Madieha Azmi, *Personal Data Protection Law: The Malaysian Experience*, 16 Info. & Comm. Tech. L. 125, 131-2 (2007). Similarly, Al-Awzai defined *Al-tagassas* as an attempt to disclose any concealed matter. 10 Ibn Abi Hatim, *Tafsir*, 3305 (1997). Other scholars such as Al-Baghawi, Al-Washtani, and Alsijistani used similar definition to describe Al-tagassas. See Eli Alshech, *Notion of Privacy in Classical Sunni Islamic* 98 (2004) (unpublished Ph.D. dissertation, Princeton University).

⁵⁴ Azmi, *supra* note 35 at 131.

⁵⁵ I will explain later in this chapter the elements of this crime.

Upon studying the evidence from the Quran and Sunnah texts, as well as classic scholars' opinions, it is clear that the protection of the dwelling is to prevent the invasion of the residents' privacy since the houses were, and are probably still, places where people expect to have more privacy than anywhere else.

First, the Quran prohibits people from entering others' homes without seeking prior permission, even if the house is unoccupied.

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). If you find no one in the house, enter not until permission is given to you: if you are asked to go back, go back: that makes for greater purity for yourselves: and Allah knows well all that ye do.⁵⁶

Al-Zamakhshari, known as an expert on *tafsir* (Quranic exegesis), explained that the rationale behind such prohibition – entering the house during the absent of its residents – is to protect what people usually conceal from others in their houses.⁵⁷

Second, several reports from the Prophet (PBUH) indicate that the rules in Islam are meant to protect what is inside the house more so than they are to protect the right of ownership (the property). Abu Huraira narrated that The Prophet (PBUH) said, "If someone is peeping (looking secretly) into your house without your permission, and you throw a stone at him and poke his eyes, you will not be blamed."⁵⁸ In a similar hadith, as-Saidi reported that a person peeped through the hole of the door of the Prophet (PBUH) and he had with him some pointed

⁵⁶ Quran, surah Al Noor (24:27).

⁵⁷ 4 MAHMOUD AL-ZAMAKHSHARI, AL-KASHAF 288 (1997). Also, Ibn Ashur emphasized that the reason behind this rule is protect what people wishes to hide from others from any disclosure. 19 IBN ASHOUR, ALTAHRIR WA ALTANWIR 201 (1994)

⁵⁸ Sahih al-Bukhari, Book 87, Hadith 26.

thing with which he had been adjusting (the hair of his head). The Prophet (PBUH) said to him, “If I had known that you were peeping, I would have thrust it in your eyes. Allah has prescribed seeking permission as a means of protection against glance.”⁵⁹ Moreover, the Prophet states, “Visitors must not stand in front of the houses’ doors when they seek permission to enter them.”⁶⁰ The Prophet (PBUH) also said, “If one’s eye has entered a private place, the person him- or herself has entered.”⁶¹

Drawing from the previous hadiths, it is evident that looking inside someone's house without permission, even if the person is located outside the property, is a punishable crime per Islamic rules. The physical intrusion is not an element of this crime.⁶² The person who looked inside the Prophet’s room deserved to be punished, even though he was standing outside the property. Allowing the resident to poke the peeper’s eye without being held responsible indicates how serious this crime is in Islam. Some Islamic scholars have suggested several requirements be met before this right (poking the voyeur’s eye) is exercised. For example, most scholars agreed that the action has to be ongoing, so if the peeper left before the inhabitant poked his eye, the inhabitant does not have the right to follow him and poke his eye.⁶³ In addition, Al-Mawardi warns not to poke out the eye of a person who peeks into a house through an open window or door.⁶⁴

⁵⁹ Sahih Muslim, Book 38, Hadith 54

⁶⁰ ALHAFID AL HYTAMI, MAJMAH ALZWEED AND MANBAA ALFAWAED 88 (Dar Alfikr Alarabi, Beirut, 1992).

⁶¹ Cited in Ahmad Atif Ahmad, *The Right to Privacy and Sunne Islamic Law: Preliminary Remarks*, Sep. 12, 2005, at http://ahmadatifahmad.blogspot.com/2005/09/privacy-and-islamic-law_12.html.

⁶² For the elements of this crime and more explanation, see Al-Jundi, *supra* note 9 at 139-153.

⁶³ Other scholars state that a warning should be giving before poking the eye. See Alshech, *supra* note 53 at 61.

⁶⁴ 17 ALI AL-MAWRDI, AL-HAWI ALKABEER 377 (1994).

In fact, if a stranger fully enters a house with his or her body, without permission, the resident would face stricter limitations before being allowed to exercise the right to attack the intruder's eye. The residents must warn the intruder to leave, and only then may they employ the least dangerous or harmful means to force the intruder to leave.⁶⁵ Al-Razi explained that if a person enters a house, the inhabitants would be aware of his or her existence and would, therefore, conceal their secrets before forcing the intruder to leave the house. On the other hand, if the person looks inside the house from a hidden place without entering the house, the inhabitants would be unaware of the person who looks into their home. Therefore, they would be less likely to conceal their private lives.⁶⁶

Third, based on Islamic jurisprudence, many classic Islamic scholars from different schools agreed that if a person builds a house that is taller than the neighbor's house, which might cause for the inside of the shorter house to be exposed, he or she is required to cover the windows of the taller house that permit one to look into the neighbor's shorter house. Moreover, a *muezzin*, a man who calls Muslims to prayer from the minaret of a mosque, is not allowed to ascend the minaret if that might expose the houses nearby, even if the minaret was built before the houses.⁶⁷

This evidence suggests that the purpose of the prohibition is to protect the secrets held within a house and not just the safety of the residents, nor ownership.⁶⁸ However, this does not mean that the property or the residents are not protected under Islamic law. Indeed, Sharia law

⁶⁵ This called “Dafe Alsael” the rules of self-defense. See 12 IBN QUDAMAH, ALMUGHNI 531 (1997).

⁶⁶ 23 FAKHR AL-DIN AL-RAZI, TAFSIR AL-KABIR 199 (1981)

⁶⁷ Alhamim, *supra* note 5 at 169.

⁶⁸ Alhamim, *supra* note 5 at 166.

protects the property and the body of the person via different areas of Islamic jurisprudence such as theft, abstraction, and assault.⁶⁹

- **The usage of technology to invade someone's house**

By analyzing the hadiths that discuss the sanctity of home, it is clear that Islam focuses on protecting the private life that exists inside the house, not the property. The hadiths give a person the right to protect his or her privacy from an intruder, even if the intruder is not physically inside the property. The crime here is exposing what is inside the house, not entering the property. Thus, any action or applied technique that violates the privacy of someone's home without permission will now be equally prohibited.⁷⁰ This principle might be applicable to today's issues having to do with technology, such as thermal imaging or cameras, being used from afar to reveal information that exists inside the house.⁷¹ Many questions surrounding the use of technology still need answers. For example, whether the inhabitants have the right to destroy the technology used to reveal their information is a question that needs to be addressed. In addition, unlike the naked eye, the technology can record and save a person's private information for an extended period. Therefore, since it is ongoing crime, it is worth considering whether the inhabitants have the right to follow the peeper and destroy the technology used to disclose information pertinent to their private life inside the house. This dissertation is not meant to answer every question regarding this matter; rather, the focus here is to examine the main principles and the comprehensiveness of these principles.

Lastly, it is important to mention that Sharia asks residents to take necessary precautions to protect their privacy; these precautions can include closing doors and covering windows.

⁶⁹ *Id* at 169.

⁷⁰ *Id.*

⁷¹ Al-Jundi, *supra* note 9 at 214.

According to Al-nawawi, if a door is wide open and someone looks through the door without entering the house, it is not a crime, so the dweller cannot defend the dwelling by throwing a stone because he or she is being *mofardh* (“careless”).⁷² Al-nawawi provided another example involving a person looking out from a higher building. In this case, the peeper is committing a crime since the dweller is not being careless. To conclude, Sharia gives the dwelling the highest protection by granting the resident the right to defend his or her privacy against violation. Sharia does, however, order the dweller to take reasonable precautions in order to be able to enjoy that level of protection. Finally, it is worth mentioning that, while looking through an open door is not a crime, it is still considered a disapproved action in Islam.

▪ **Private correspondence**

As discussed previously, several hadiths clearly state that looking inside a house is prohibited, but one might raise the question, what about spying on a house by listening? The classical Islamic scholars have indeed raised this question when they discuss previous reports: “Allah has prescribed seeking permission as a means of protection against glance” and “If someone is peeping (looking secretly) into your house without your permission, and you throw a stone at him and destroy his eyes, you will not be blamed.”

The scholars agree that listening to conversations inside a house is certainly forbidden by other reports. Ibn Abbas Narrated that The Prophet (PBUH) stated, “If a person listens to the talk of those who do not wish to be heard, then molten lead will be poured into his ears on the Day of Resurrection.”⁷³ This Hadith establishes the prohibition of spying by listening to a conversation between people who do not want to be heard. Unlike the hadiths that refer to “looking inside a house,” this hadith does not mention the place where the confidential conversation takes place.

⁷²10 ALNAWAWI, RAWDAH ALTALIBIN WA OMDAH ALMUFTIN 193 (1991).

⁷³ Sahih Al-Bukhari, Book 18, Hadith 34.

Though scholars agree that listening to people speaking inside a house is a crime, they disagree regarding the seriousness of this crime. Is it the same as looking into a house without permission? In other words, can the residents of the house thrust at the ear of the hidden listener?

Most of the classical Islamic scholars from different schools, except for a few Shafi, tend to take the hadith at face value rather than expand its meaning to include spying by listening. In general, the scholars hold that looking inside a house reveals more information than just listening to people's conversations does.⁷⁴ Thus, inhabitants are not entitled to the same rules as if someone violates their privacy by looking inside their house because the two conditions are not compatible. This does not mean that the law, in this case, will not punish the listener for his crime. In fact, the ruler is required to punish anyone who commits this crime by issuing a law or by giving the judges the right to penalize the violator.

There are some scholars, however, who disagree with the majority. These scholars believe that listening to people speak inside their homes can be just as much an invasion of privacy and therefore just as dangerous as looking at them without their permission. It depends on the situation of the residents. Thus, according to Al-himim, listening to people speaking inside their homes is equivalent to looking at them, and the hadith is meant to protect the secrets of people inside their homes from any kind of invasion or from being revealed through any means. This is relevant to today's technologies that include small recording devices that might effectively reveal every conversation that takes place inside a house.⁷⁵

- **Personal letters**

The prohibition of spying includes looking at personal letter, notes, and confidential documents without explicit permission. The prohibition stands on a hadith that warns anyone

⁷⁴ Al-Jundi, *supra* note 9 150.

⁷⁵ Alhamim, *supra* note 5 at 286.

who looks at a private letter. The hadith reads, “One who looks at his brother’s letter without his permission is essentially looking into the fire of Hell.”⁷⁶

Although this hadith is *daif* (“weak”), scholars tend to accept its meaning, which fits with the Islamic principle of prohibiting spying in general.⁷⁷ Comparing looking at a letter with looking into Hell is a means of demonstrating the seriousness of the prohibition.⁷⁸ Letters and messages sent by email, fax, and post are considered documents that are associated with trust (*amanah*) in Sharia.⁷⁹ Violation of *amanah* is a punishable offense if either the sender or the receiver is harmed by the breach of trust and the disclosure of confidential information.⁸⁰ In addition, the violation might result in financial compensation, penal sanctions, or both as the last section of this chapter will explain in details.

- **Spying on public places**

As discussed previously, Sharia law protects the privacy of those who are within their dwellings by prohibiting any actions that could expose details regarding their private lives. Similarly, Sharia law offers protection regarding personal letters, notes, and emails, and prohibits any kind of disclosure of the details of these documents without proper permission. A reasonable

⁷⁶ MOHAMMAD HASHIM KAMALI, THE DIGNITY OF MAN: AN ISLAMIC PERSPECTIVE 64 (2002). *See also* MOHAMMAD HASHIM KAMALI, THE RIGHT TO LIFE, SECURITY, PRIVACY, AND OWNERSHIP IN ISLAM 193 (2008).

⁷⁷ *Id.*

⁷⁸ Alhamim, *supra* note 5 at 376.

⁷⁹ *Amanah* (Trust) in Sharia has a broad meaning that includes both moral and legal aspects. Some Sharia scholars believe that the fine line between the moral and the legal aspect is the intention of both parties. For the *amanah* to be legally binding (i.e., the one who lost the *amanah* will be liable), both parties have to come to an agreement, explicit or implied, to keep the information, or anything secret, away from other. The moral meaning of *amanah*, however, is when someone happens to find something or know some information that should be secret without any sort of agreement with the other party. The person in this case is still morally required to keep the information secret but he or she is not liable for losing the information or the thing. The classic example given by some Sharia scholars is that if a wind moved a cloth from one house to another, the person who found the cloth in his or her house is not legally liable because there is not an agreement between the parties. *See* Alhamim, *supra* note 5 at 303-306.

⁸⁰ Kamali, *supra* note 76 at 193.

question might arise then about the privacy in public places. Does Sharia law recognize an individual's right to privacy in public places?

Drawing from the hadiths and Islamic jurists' opinions, it is evident that Sharia differentiates between violation of privacy in public places that results from either looking at or listening to another.⁸¹

- **Spying on public places by looking**

Islam allows a person to physically defend his or her privacy against a violator who looked inside the individual's dwelling, provided the following criteria are met: 1) the resident must be inside his or her dwelling, 2) the resident must take reasonable precautions to cover the windows of his or her house, and 3) the violation must be occurring at the time.⁸² Without any textual evidence from the Quran or the Sunnah that specifically criminalizes the violation of privacy in public places that results from one person looking at another, we are left with the Islamic general prohibition of spying. For example, The Prophet (PBUH) instructed his Companions to avoid sitting on roadsides unless they will lower their gaze, so that you may not stare at unlawful things.⁸³

This hadith contains some general guides and morals, which are not, from the modern legal point of view, a law. In fact, some Islamic scholars have used hypothetical situations to emphasize this idea of violating privacy in public places. According to Alnawawi, if a person sits on the road without covering his or her private parts, that person has no right to physically

⁸¹ Alhamim was the first to notice this difference in his book. *See* Alhamim, *supra* note 5.

⁸² Al-Jundi, *supra* note 9 at 141-161.

⁸³ Abu Said Al-Khudri said, The Prophet (PBUH) said, 'Avoid sitting on roadsides.' His Companions said, 'O Messenger of Allah (PBUH), there is no other alternative but to sit there to talk.' Thereupon The Prophet (PBUH) said, 'If you have to sit at all, then fulfill the rights of the road.' They asked, 'What are their rights?' Thereupon he said, 'Lowering the gaze; refraining from doing harm to others, responding to greetings, and commanding the good and forbidding the evil.' Al-Bukhari and Muslim, Book 18, Hadith 113.

defend him- or herself against anyone who looks at him or her.⁸⁴ Further, according to Ibn almrzban, if a person enters a mosque (i.e., a public place) and exposes his or her private parts after closing the door, then that person has no right to physically defend him- or herself by, for example, throwing stones at a person who looks at him or her because the exposed individual is not within his or her own home.⁸⁵ As such, it is clear that the Sharia does not permit one to physically defend his or her right to privacy while he/she in public space. While Sharia does prohibit the violation of another's privacy by looking at him or her, regardless of where the act occurs, the act is not a punishable crime since an individual has no expectation of privacy in a public space.

- **Listening to private conversations in public places**

Unlike the hadiths that proscribe invading others' privacy by looking at them while they are within their private places, several hadiths criminalize listening to people without specifying whether the conversation must take place in a public or private area. For instance, Ibn Abbas stated, "The Prophet (PBUH) said, 'Whoever listens to people's conversations when they do not want him to do so will have molten lead poured into his ears on the Day of Judgment.'"⁸⁶ Additionally, Saeed alkhadari said, "One day, when I passed by Ibn Omer⁸⁷ while he was talking to someone, as I approached him, Ibn Omer pushed me on my chest and said to me, 'If you find two individuals talking to each other, do not approach them until you seek permission.'" Ibn

⁸⁴ Alnawawi, *supra* note 72 at 192. See also 9 Ibn Qudamah, *Supra* at 187.

⁸⁵ *Id*

⁸⁶ Sahih Al-Bukhari, chapter 18, Hadith 34.

⁸⁷ "Ibn Omar (ca.614-693) was the son of the second Caliph Omar ibn Khattab. He was a prominent authority in Hadith and law. As a transmitter of Tradition, he has been regarded as the most scrupulous in neither adding to nor omitting anything from the *hadiths* narrated by him." L. Veccia Vaglieri, 'Abd Allāh b. 'Umar b. al-Khattāb, in Encyclopaedia of Islam (P. Bearman et al. eds., 2nd ed. 2012) available at http://referenceworks.brillonline.com.proxyiub.uits.iu.edu/entries/encyclopaedia-of-islam-2/abd-allah-b-umar-b-al-khattab-SIM_0067.

Omer continued, "Have you heard what the Prophet (PBUH) said? 'If two people were secretly talking to each other, no one should enter between them until he or she seeks permission.'"⁸⁸

It is clear that Ibn Omer was talking in a public area when Saeed approached him. This hadith indicates that the prohibition of spying by listening to confidential conversations is not limited to private places, and people can expect privacy of this sort even when they are in public. Ibn Hajar notes that there is an exception to this; one is excused from the threat stated in the hadith (i.e., "will have molten lead poured into his ears on the Day of Judgment") if he or she happens to be in a place where two people are talking loud enough that it is clear – per their volume – that the conversation is not private.⁸⁹

When analyzing the Sharia rules and regulations regarding privacy in public places, one must differentiate between listening and looking. All of the evidence from the Quran and Hadith, which specifically address the invasion of privacy by *looking*, connect the invasion of privacy to taking place within a private dwelling. However, protection against an invasion of privacy by *listening* is applicable whenever the conversation appears to be private no matter whether the conversation occurs in a public or private place.

Today, based on the general prohibition, using any type of technology to listen to any conversation that appears to be confidential is prohibited, no matter where does that conversation took place, under Sharia law. There is a dilemma, however, associated with the use of technology to watch or track people in public places. To clarify, when Islam began, people could anticipate the range where they might be exposed to the public naked eyes, which made it difficult to argue that a person could reasonably expect privacy in a public place. Thus, Sharia limits its protection against an invasion of privacy by *looking* to people who are in private places

⁸⁸ 2 ALBUKHARI, ALADAB ALMOFRAD 580 (1997). See also Alhamim, *supra* note 5 at 153.

⁸⁹ Alhamim, *supra* note 5 at 154.

and do not expect to be seen. With regard to invasion of privacy by *listening*, however, Sharia did not limit its protection to a private place because people, such as Ibn Omer, can have conversations in public areas and still expect privacy. Today, as technology continues to advance quickly, it is very difficult to anticipate what actions new technologies will be capable of performing. For example, if a person does not have an expectation of privacy regarding his or her short movements in public places because everyone can notice his/her short movement, what about the use of technology, such as street cameras, GPS, or automatic license plate recognition tools, which have the ability to record people's movements over extended periods. In this case, an individual's expectation of privacy might be reasonable.

This raises a question: Can people have an expectation of privacy in public places? What is the rule here per Sharia? Attempts to prescribe tracking movements in public places are almost nonexistent in the legal sources the author of this dissertation consulted.

➤ **Seeking permission**

The individual's home has always been regarded as his or her private preserve and an exclusive place where he or she feels safe from the intrusion of others. Thus, protecting people's homes has always been central to the right to privacy in both the old and modern constitutions and legislations around the world. In Sharia law, it is evident that most of the verses in the Quran and the hadiths, and the discussions held among the Islamic jurists, emphasize the need for people to seek permission before entering others' homes. Islamic scholars, however, using the fourth source of Sharia law, *qiyas* ("analogy"), extended some of these rules to spaces beyond the house.

- **Seeking permission before entering someone’s home**
 - **What is “home”?**

The answer to this question is the cornerstone of the right to privacy in Sharia. The meaning of private home or dwelling (*maskan, manzil, bayt*) tends to be more a concept than a physical structure of a particular kind.⁹⁰ For example, a private dwelling can mean a traditional home or an apartment that has clear boundaries and walls, or it can mean another type of structure that might be fragile or slight in nature and thus may fail to provide a physical barrier against intruders. A private dwelling might also have been built in a place that is not owned by its resident.⁹¹ According to the Quranic view, a private dwelling is a place where one resides and where others are not allowed to enter without permission.⁹²

To explain the Arabic word *maskan* (“home”), Al-Isfahani wrote that it means a place where one finds safety from fear, assurance of one's property and honor, and a place where one feels comfort, privacy, and peace.⁹³ Similar Arabic words *manzil* and *dar* express the same meaning, and they all signify a place in which one actually lives, regardless of whether or not the space is considered a “proper” living space or whether the occupancy is temporary or permanent.⁹⁴ The physical structure of the house and the materials from which it is made are irrelevant; whether weak or strong, a cave or a tent, a mobile home or a caravan, every home enjoys the same protection, regardless of its location, monetary value, or other features.⁹⁵

⁹⁰ Kamali, *supra* note 76 at 162.

⁹¹ Some scholars state that the elements of the ‘*maskan*’ are occupancy, and protection from sun and rain the eyes of the passers-by. 6 IBN HAZIM, ALMUHALA BALATHAR 156 (Dar Ibn Hazim 2006).

⁹² Kamali, *supra* note 76 at 162.

⁹³ ALASFHANI, ALUFRADAT 236 (Dar ALkalam 2009)

⁹⁴ HUSSAN ALJUNDI, SHARH QANON ALOQUOBAT 577-578 (2002).

⁹⁵ Ibn Hazim, *supra* note 91 at 156.

Additionally, Some scholars extend the concept of home (bayt) to private boats and car that is under custody (*hirs*).⁹⁶

For the Shared places, the requirement that inhabitants who live in a shared place seek permission from one another is dependent on the structure of that place. First, if the place has no separate compartments, all inhabitants are equally permitted to enter the place without seeking permission.⁹⁷ Common rooms located within dormitories, shops, and hospitals are other examples of places where the inhabitants are not required to seek permission upon entry. Second, if the shared place does have separate compartments, the residents are required to seek permission before entering others' private spaces such as a room in the dorm or hotel.⁹⁸

- **The role of General Custom**

According to Al-Hmaiem, the fine line between a public space and a private space has to do with seeking permission.⁹⁹ Private places are where people customarily seek permission before entering, while a public place, such as a mosque, is where people usually enter without seeking permission.¹⁰⁰ Other scholars have also discussed the decisive role of general custom in this context. Al-Sulami, one of the Shafi jurists, believed that the general custom should be the basic indicator by which to differentiate between public and private place. There is, customarily, no need to obtain permission to enter public baths, mosques, or courthouses once their doors open to the public, but this does not eliminate the need for obtaining permission to enter certain parts of such premises, which may be private, and general custom determines them as such. One

⁹⁶ Quran used bayt when referring to ship of the Prophet Noah "My Lord, forgive me and my parents and whoever enters my house (bayt) a believer." Surah Noah (17:28). See Kamali, *supra* note 76 at 175.

⁹⁷ Kamali, *supra* note 76 at 169.

⁹⁸ Al-Jundi, *supra* note 9 at 64.

⁹⁹ Al-Hamiem is the author of one of earliest book that talks about privacy in Islam as a right by itself.

¹⁰⁰ Mujahid said, "Ibn 'Umar did not ask permission to enter shops in the market." Al-Adab Al-Mufrad, Book 43, Hadith 48.

place, such as a store with a small private room in the back, might be public in some parts and private in others. Other places, such as a hotel room, might be public for a period and private at other times. In a hotel, an occupied room is a private place, and one must seek permission before entering this space.¹⁰¹ Permission is based on either general custom or the permission granted by the inhabitants. If the general custom is not known or if one is in doubt regarding it, then a potential visitor needs to secure permission before entering a space.¹⁰²

Two factors make the general custom central whenever discussing privacy in Islam. First, the right of privacy is, to some extent, influenced by what people expect is included in this right or what they deem to fall beyond this right. Second, what makes the situation more complicated in Sharia law is that Islam is a religion that originated in the Arabic peninsula at the start of the 7th century and spread around the world, mostly in Asia and Africa. This might rationalize the absence of a comprehensive definition of privacy, or of a consensus among scholars of comparative law about essential elements of the right to privacy. These factors necessitate that general custom play central role in defining the right to privacy in Islam.

▪ **The purpose of seeking permission**

The specific purpose behind the command to ask permission before entering a person's private life or space is stated in several hadiths. For example, Sahl bin Saad stated, "The Prophet (PBUH) said, 'Seeking permission to enter [another person's house] has been prescribed to restrain the eyes [from looking at something at which we are not supposed to look].'"¹⁰³ One can infer from "to restrain the eyes" and "to escape from the look of an eye" that the purpose of

¹⁰¹ Alhamim, *supra* note 5 at 144.

¹⁰² SULAMI, QAWAID AL-AHKAM, (MAKTABAT ALKLYAT ALAZHARIAH) 285 (1991).

¹⁰³ Al-Bukhari, Book 79, Hadith 6241.

requiring permission in Sharia is to give an individual control over his or her private life against unwanted intervention.¹⁰⁴ Property ownership is protected under a different set of rules.

- **Seeking permission is required**

- **General permission**

‘O you who believe! Enter not houses other than your own, until you have asked permission and greeted those in them, that is better for you, in order that you may remember’¹⁰⁵

This Quranic verse indicates that all Muslims must seek permission before entering others’ houses. The Muslim jurists reached a consensus that seeking permission before entering someone’s home is obligatory for every adult who is not *mahram* (“an unmarriageable person”), but they disagreed regarding whether this is obligatory or merely preferable for the mahram.¹⁰⁶

The majority opinion is that a maharam is subject to the same obligation as any other adult.

Alshfi and Maliki based their shared opinion on several reports stating that a man must ask permission before entering the house of his mother or sister.¹⁰⁷

- **Special permission/aggravating circumstances**

O ye who believe! Let those whom your right hands possess, and the [children] among you who have not come of age ask your permission [before they come to your presence], on three occasions: before morning prayer; while ye doff your clothes for the noonday heat; and after the late-night prayer. These are your three occasions of undress; outside of those times, it is not wrong for you or for them to move about attending to each other. Thus does Allah make clear the signs to you, for Allah is full of knowledge and wisdom. But when the children among you come of age, let them [also] ask for permission, as do those senior to them [in age]. Thus does Allah make clear His signs to you, for Allah is full of knowledge and wisdom.¹⁰⁸

¹⁰⁴ Another report, a man stood front of the door of the Prophet to ask permission The Prophet (PBUH) said to him: Away from it, (stand) this side or that side. Asking permission is meant to escape from the look of an eye. Sunan Abi Dawud, Book 43, Hadith 402.

¹⁰⁵ Quran, Surah Al Noor (24:27).

¹⁰⁶ Alhamim, *supra* note 5 at 191.

¹⁰⁷ Id. Also, Ata Ibn Yasar reported that the Prophet (PBUH) was questioned by a man who said, "Messenger of Allah, shall I ask permission of my mother to enter?" He said, "Yes " The man said, "I live with her in the house." The Prophet (PBUH), said: "Ask her permission." The man said, "I am her servant." the Prophet (PBUH), said, "Ask her permission. Do you want to see her naked?" He said, "No." He said, "Then ask her permission." Muwatta Malik, Book 54, Hadith 1766

¹⁰⁸ Quran, Surah Al Noor 28 (24:28).

Under certain circumstances, Islam goes behind closed doors and regulates the rules related to seeking permission among family members who live under the same roof. Two remarkable features of this verse are the extension of the rules of privacy to members of one's own family and household, and the assigning of certain times of the day as times of privacy and rest during which others, including relatives, servants, and children, are commanded to seek permission before entering a private space.¹⁰⁹ Commentators have explained that the three periods specified in the verse, namely early morning, noontime, and late evening, were customary times of rest for Arabs. This verse states that *istidhan* ("seeking permission") is a requirement among family members, children, and servants only during the three times specified, but not during the longer intervals in between. The distinction between this verse and the one discussed earlier is that one is specific and the other is general. The first one, which states, "O you who believe! Enter not houses other than your own, until you have asked permission and greeted those," laid down general rules of *istidhan* that address every individual, whereas the second verse, which states, "O ye who believe! Let those whom your right hands possess, and the [children] among you who have not come of age ask your permission," issued rules to certain family members, commanding them to seek permission during specific times when people who live in the house usually need more privacy. The scholars examined in depth when the three times begin and end. It is no longer critical, however, to discuss these three specific times because the general custom and the design of houses have changed significantly. Ibn Abbas¹¹⁰

¹⁰⁹ Kamali, *supra* note 76 at 172.

¹¹⁰ Ibn Abbas is considered one of the greatest scholars, if not the greatest, of the first generation of Muslims. He was the father of Quranic exegesis; at a time when it was necessary to bring the Quran into accord with the new demands of a society which had undergone a profound transformation, he appears to have been extremely skillful in accomplishing this task. L. Veccia Vaglieri, 'Abd Allāh b. al-'Abbās, in *Encyclopaedia of Islam* (P. Bearman et al. eds., 2nd ed. 2012) available at http://referenceworks.brillonline.com.proxyiub.uits.iu.edu/entries/encyclopaedia-of-islam-2/abd-allah-b-al-abbas-SIM_0035.

explained that the purpose of these rules was to protect people who had neither curtains nor curtained canopies in their houses, so that a servant, a child or a female orphan of a man would not enter a private space while the man was having sexual intercourse with his wife.¹¹¹

There are three primary points that serve as the key takeaway regarding this verse and modern life. First, the fact that Sharia law regulates relations within one's home among family members, including children, to guarantee that the inhabitants enjoy a high level of privacy is suggestive of the value Sharia places on the right to privacy. Second, the rules associated with the right to privacy in Islam are notably influenced by *urf* ("general custom"), which helps these rules to sustain longer and to be applicable among different societies. Third, Sharia adheres to the notion that one should be offered a greater level of protection regarding individual personal space when he or she needs and expects increased privacy under certain situations (i.e., the three specified times outlined in this verse). Sharia required family members to seek permission only at certain times when the individual, the subject, expected to be left alone to rest or to remove his or her clothing. This concept exists among many of the contemporary privacy protection laws around the globe, where they give greater protection to so-called "sensitive information" such as medical records and information about children.

¹¹¹ Ikrimah said: A group of people from Iraq said: Ibn Abbas, what is your opinion about the verse in which we have been commanded whatever we have been commanded, but no one acts upon it? The word of Allah, Most High, reads: "O ye who believe! Let those whom your right hands possess, and the [children] among you, who have not come of age, ask your permission (before) they enter your presence on three occasions: before Morning Prayer, while you are undressing for the noonday heat, and after late-night prayer. These are your three times of undress; outside those times it is not wrong for you or for them to move about." Al-Qanabi recited the verse up to "full of knowledge and wisdom." Ibn Abbas said: Allah is Most Clement and Most Merciful to the believers. He loves concealment. The people had neither curtains nor curtained canopies in their houses. Sometimes a servant, a child or a female orphan of a man entered while the man was having sexual intercourse with his wife. So Allah commanded them to ask permission in those times of undress. Then Allah brought them curtains and all good things. But I did not see anyone following it after that. Sunan Abi Dawud, Book 43, Hadith 420.

- **How to seek permission**

Sharia law in several Quranic texts and hadiths discusses the ways in which people should seek permission. Upon analyzing the Quranic texts and hadiths, it is evident that there are two ways to seek permission under Shari law: explicit and implied permission.

- **Explicit permission**

Most of the Quranic texts and hadiths discuss explicit permission, which, per Islamic principles, is perhaps the preferable way to seek permission. Explicit permission involves a direct invitation extended via any means – an oral or written invitation, or another type of action that makes it clear that an invitation is being extended.¹¹² Sharia law provides some instructions about how to seek permission. While some of these instructions are considered preferable or Sunnah (not obligatory), addressing them is important in order to clarify the meaning of explicit permission in Sharia.

First, Islamic jurists agree that greeting a home's inhabitants before or after one seeks permission is preferable (Sunnah). The Quran emphasizes the importance of greeting inhabitants prior to entering dwellings.¹¹³ The verse states that those seeking permission should extend greetings before going into others' homes: "O you who believe! Enter not houses other than your own, until you have asked permission and greeted those in them, that is better for you." In addition, some hadiths explain that the greeting should be extended before permission is sought.¹¹⁴ Further, the hadiths indicate that the act of greeting a home's inhabitants is additional

¹¹² IWAD MUHAMMAD, DERASAT FI ALFIQH ALJNAI AL-ISLAMI 116 (2010).

¹¹³ Alhamim, *supra* note 5 at 197 (2003).

¹¹⁴ Sharia Scholars agree that greeting is a Sunnah (not obligatory). However, they disagree about the time of the greeting whether before or after seeking permission. According to Alnawawy, the majority believe that greeting should be before asking permission. Narrated Rib'i: A man of Banu Amir told that he asked the Prophet (PBUH) for permission (to enter the house) when he was in the house, saying: May I enter? The Prophet (PBUH) said to his servant: Go out to this (man) and teach him how to ask permission to enter the house, and say to him: "Say: Peace be upon you. May I enter?" The man heard it and said: Peace

to the act of seeking permission, and that these two acts are not the same single act. However, unlike the requirement that entails prospective visitors seeking permission, the directive to greet inhabitants before entering their homes or spaces includes the owner of the house.¹¹⁵

The second directive is to make oneself known before seeking permission. Jabir wrote, “I went to the Prophet (PBUH) and knocked at the door [to seek permission]. He asked, ‘Who is there?’ I said, ‘I.’ He repeated, ‘I, I!’ as if he disliked it.”¹¹⁶ Making oneself known is an important step to clearly letting the resident know who is seeking permission, and this in turn allows the resident to decide whether to grant the individual permission. Today, many information privacy laws state that individuals have the right to know what companies are going to use their information before permission is granted.

Third, an individual may not ask more than three times to enter. Abu Musa Al-Ash'ari stated, “The Prophet (PBUH) said, ‘Permission is to be sought thrice. If it is accorded, you may enter; otherwise, go back.’”¹¹⁷ The purpose of this directive, as indicated by Abu Hurayra, is to initially alert the homeowner of one’s presence, to subsequently allow the homeowner and other inhabitants the time necessary to prepare themselves for a visitor and to change into appropriate attire, and finally, to obtain a reply about whether or not the prospective visitor may enter.¹¹⁸

Islamic jurists disagreed regarding whether this meant that a person must seek permission three times every time he or she wishes to visit or the person may seek permission a maximum of three

be upon you! May I enter? The Prophet (PBUH) permitted him and he entered. Sunan Abi Dawud (138) Chapter: How is permission to be sought), Book 43, Hadith 405. *See* Alnawawi, Sharh Saheh Muslim, book 14, hadith 136.

¹¹⁵ “So when you enter houses, salute one another (Literally: salute yourselves) with a greeting from the Providence of Allah, blessed and good”. MUHAMMAD IBN JARIR AL-TABARI, TAFSIR AL-TABARI [EXPLANATION OF TABARI], *available at*

http://library.islamweb.net/newlibrary/display_book.php?idfrom=3561&idto=3561&bk_no=50&ID=3586

¹¹⁶ Al-Bukhari and Muslim. Book 6, Hadith 33

¹¹⁷ Al- Bukhari and Muslim, Book 6, Hadith 26

¹¹⁸ 3 AL-SABUNI, MUKTASAR TAFSIR IBN KATHER, 282 (1981). *See also* Al-Jundi, *Supra* note 9 at 87.

times; however, the majority believe that it is not required to repeat the request three times if permission was granted upon the first or second request.¹¹⁹

Another practical question has to do with whether it is permissible to seek permission more than three times. Al-Qortoby answered this question by taking the direct meaning of the aforementioned hadith, which states that requests for permission are limited to three.¹²⁰

However, other jurists, such as Ibn Al-arabi, allow for an exception to prospective visitors who believe that they have not been heard; these individuals are permitted to make more than three requests.¹²¹

- **Implied permission**

Sharia law recognizes implied permission as another way to express permission. Awad Mohammad defined implied permission by stating that it is when the permission is derived from a reasonable interpretation of certain actions or statements that usually serve as means of granting permission to others.¹²² Awad presented some situations and places wherein permission is indirectly granted. For example, places whose specific purposes cannot be fulfilled unless visitors are permitted to enter without actively seeking permission must grant implied permission to enter; such places include stores, hospitals, courts, and mosques. Furthermore, the existence of a close relationship might allow for implied permission to be sufficient if the general custom usually permits. For example, a son may enter his parents' home without seeking explicit permission except during certain times or if he seeks entry to certain rooms.¹²³

¹¹⁹ Al-Jundi, *supra* note 9 at 89.

¹²⁰ 15 AL-QORTOBY TAFSIR AL QORTOBY 191 (1964). Also, Ibn Qayyim agrees that the hadith limits the request for permission to three times without any exceptions. 2 IBN QAYYIM, ZAD ALMAAD 430 (1979).

¹²¹ 3 IBN AL-ARABI, AHKAM AL-QURAN 1350 (3ed ed 1958). Also, Al-jundi agrees with this option. Al-Jundi, *supra* note 9 at 91.

¹²² Muhammad, A. *Derasat Fi alfiqh aljnai al-islami*, 117 (2010)

¹²³ *Id.*

Implied permission depends largely on the general customs. This could be seen in the hadith in which Ibn Masud stated, “The Prophet (PBUH) said to me, ‘The sign that you have been permitted to come in is that the curtain is raised or that you hear me speaking quietly until I forbid you.’”¹²⁴ Moreover, another example of implied permission is the act of being invited. Abu Hurayra states that the Prophet (PBUH) said about a man being invited, "It is his permission."¹²⁵

The first hadith provides an example of a specified sign given by the prophet (PBUH) assigned as an indicator of permission. This arrangement was between the Prophet and Ibn Masud. The second hadith, however, presents an example of a general custom, when the invitation alone is considered permission to enter the place.¹²⁶ The general custom varies among societies.¹²⁷

▪ **The scope of the permission**

It is critical to identify the scope of any granted permission to be able to determine whether someone has gone beyond that of the permission and has therefore violated another’s privacy. The scope of the permission depends on two limitations: personal and in-rem.

• **Personal**

The permission is limited to certain individuals. This can be broad to include everyone such as a public store or narrowed to name only particular people in exclusion of others.¹²⁸

• **In-rem**

¹²⁴ Sahih Muslim, Book 39, Hadith 21, Chapter: It Is Permissible To Give Permission To Enter By Raising The Curtain Or Giving Some Other Sign.

¹²⁵ AL-ADAB AL-MUFRAD, Book 43, Hadith 24. AlBukari named the chapter “Chapter: If a man is invited, should he ask permission to enter”.

¹²⁶ Alhamim, *supra* note 5 at 207-208.

¹²⁷ For example, in some public places there are restricted areas for employees who work in that place.

¹²⁸ Alhamim, *supra* note 5 at 205.

The permission is limited to a place whose inhabitant has permitted others to enter. The Islamic jurists discussed the scope or the range of that limited area under the elements of theft.¹²⁹ In short, the permission can be general or special. General permission is given when the inhabitant allows another to enter any place in the house, whereas special permission is given when the occupant permits a person to be in only a limited area (e.g., giving a guest permission to be in the living room).

▪ **The authority to give permission**

An element of the validity of the permission is to be issued by a person who has authority to grant such permission. The Islamic jurists have discussed two questions pertinent to this matter. First, does the wife have the right to give someone permission to enter her husband's house? Second, do the children and those who work and live within the house have the right to give permission to others?

The following scenarios address or define the limitations regarding the first questions:

1. The husband has given explicit authority to his wife to grant permission. This authority could be limited to certain individuals or it could be general and thus permit the wife to invite in anyone she wants.
2. The husband does not give explicit authority. In this case, the wife should do what she reasonably believes her husband would say or do. Thus, if she thinks that her husband would not mind letting a given person into his house, she can permit that person to enter. Abu Hurairah noted that the Prophet (PBUH) said, "It is not lawful for a woman to allow anyone to enter the husband's house without his permission."¹³⁰

¹²⁹ The degree of penalty for the crime of theft varies depending on the place the money or the thing that being taken.

¹³⁰ Al-Bukhari and Muslim. Book 1, Hadith 282.

3. The husband explicitly refuses to grant permission to certain individuals. In this case, the wife does not have the authority to allow these people to enter the house unless these prohibited individuals are her parents or relatives.¹³¹

In general, Islam gives the husband the right to decide whether to give his wife a specific or general and implied or explicit authorization to allow individuals into his house. The reason behind giving the husband the right to grant permission or not is unclear; it may be because he is the husband, or it may be because he supposedly owns the house. Alnawawy reasoned that the husband has the right to allow or disallow anyone because he owns the house.¹³² This leaves a question unanswered: What if the wife owns the house? Does she still need authority from her husband before letting anyone into her house?

With regard to the second question, workers who live in the house and the children who have not yet attained puberty do not have the right to grant permission to anyone because they do not have legal authority.

➤ **Information pertaining to others**

Sharia regulates the disclosure of others' information via two main concepts: first, the proscription of revealing others' information that, when revealed, would prove deleterious to them (*sater al-awrat*); second, the instruction to keep others' confidential information in general (*kitman al-sir*).

¹³¹ Most of the jurists believe that she has the right to see her parents. Islamweb.net, *hakam 'iidkhal ahd alzawjayn shakhsaan lilbayt dun 'iidhn alakhar* (May 2, 2010).

[http://fatwa.islamweb.net/fatwa/index.php?page=showfatwa&Option=FatwaId&Id=135569.](http://fatwa.islamweb.net/fatwa/index.php?page=showfatwa&Option=FatwaId&Id=135569)

¹³² Islam Question & Answer, *ma hi alhalat alty yjb ealaa alzawjayn muraeatiha fi alaistidhan ealaa dukhul, 'aw edm dukhul, almaharim 'aw ghyr almaharim fi manzil alzawjia?* (Aug. 7, 2008), [https://islamqa.info/ar/112048.](https://islamqa.info/ar/112048)

ALNAWAWI, ALMUNHAJ SHARAH SAHIH MUSLIM BIN ALHUJAJ v.7 at 115 (Dar 'iihya' alturath allearabii – bayrut 1392).

- **Concealing others' damaging information (*sater al-awrat*)**

Keeping others' information that could prove damaging if it were revealed is one the main themes of the Sunnah, and the instructions of the Prophet (PBUH) on this matter are forceful in that they are not limited to moral guidance but include legal ruling. Jurists have found that much of what the Sunnah has to say regarding this issue is legally imposed, and they have based some of their conclusions on it.¹³³

The Prophet (PBUH) said, "Whoever covers up (*sater*) the fault of a Muslim, Allah will cover up his fault on the Day of Resurrection."¹³⁴ In addition, the Prophet (PBUH) threatened anyone who tries to expose others' secrets by stating that God will punish them.¹³⁵

Several other hadiths emphasize this and encourage people not to disclose others' hidden faults. A common phrase that is used repeatedly throughout these hadiths is "*sater al-awrah*." The accurate translation of the word "*sater*" is "to cover," whereas "*al-awrah*" has a broad meaning which includes any flaw or fault that people would generally have a strong urge to conceal. Per the Islamic texts, the Quran and Sunnah, *al-awrah* also used to indicate some physical parts of a person's body, such private parts, or non-physical acts such as religious misconduct.¹³⁶ Since the purpose of this chapter is to examine to what extent the law protects the individual's personal information, it is vital to clarify the generality of the previous hadiths using practical examples that illustrate the legal extent of these hadiths. Providing two practical examples from Islamic jurisprudence will illustrate how Islamic jurists and classical scholars have understood and applied these hadiths such that they served as more than moral guides.

¹³³ Kamali, *supra* note 76 at 200 (2008).

¹³⁴ Al-Bukhari and Muslim, Book 1, Hadith 233.

¹³⁵ "For indeed whoever tries to expose his Muslims brother's secrets, Allah exposes his secrets wide open, even if he were in the depth of his house." Jami' at-Tirmidhi 2032, Book 27, Hadith 138 Grad: Hassan.

¹³⁶ Kamali, *supra* note 76 at 202.

First Example: Testimony

A prominent example of such restrictive legislation relates to testimonies. The Quran imposes a duty to all Muslims to testify in court and warns them against withholding their testimonies.¹³⁷ Most Islamic scholars from different Islamic jurisprudence schools agree, however, that there are conditions under which a witness could be released from his duty to testify against a transgressor, and that under some conditions, he is even obliged to do so. The Hanbalis, for example, permits a witness to abstain from testifying when he or she has witnessed a transgression that does not violate another person's interest. Still, he or she must testify in all other circumstances. Hanafi and Shafi scholars gave a witness the choice of not testifying if the act requires a Hadd, except in the case of theft.

In fact, theft is a perfect case wherein there is a fine line between the duty to testify and the requirement to conceal others' faults (*seter al-awrat*). Theft is one of the Hudud in Islam that is considered a violation against God and man.¹³⁸ According to Al-Sarkasi, it is preferable for the witness to withhold his testimony if the theft returns what he or she stole.¹³⁹ In addition, Al-Sarkasi suggests that if the theft did not return what he or she stole, the witness could testify that he or she "took" instead of "stole." Thus, the stolen items or goods will be returned to where they belong without additional information regarding the theft being disclosed.¹⁴⁰

As these examples indicate, despite the fact that Quran requires a witness to testify and disclose incriminating information in all cases, Shariah gives exceptions to this rule. A witness is

¹³⁷ "Do not conceal testimony, for whoever conceals it - his heart is indeed sinful, and Allah is Knowing of what you do." Quran, Albaqarah, (3:283). "let not the witnesses refuse when they are called upon" Quran, Albaqarah, (3:282).

¹³⁸ In contrast, the adultery is a punishable crime that violates only the God.

¹³⁹ S. IDRIS, KTMAN ALSR WIFSHAOUH FI ALFKH ALISLAMI [CONFIDENTIALITY AND DISCLOSURE IN ISLAMIC JURISPRUDENCE] 119 (1997).

¹⁴⁰ *Id.* at 120.

allowed – even encouraged – to withhold his testimony, and in some cases, he is prohibited from testifying. These exceptions were made, Al-Marghinani explains, to protect the transgressor against unnecessary exposure (hetk).¹⁴¹

Second Example: The Privacy of the Deceased Person

Another example from the Islamic jurisprudence that illustrates the implication and the extent of the obligation to conceal information that could harm others once it is revealed pertains to information regarding a deceased person. Sharia extends its regulations regarding not revealing damaging information about others to those who are deceased. In fact, several prophetic hadiths were specific with regard to revealing damaging information about the deceased. According to Aisha, the Prophet (PBUH) said, “When your companion dies, leave him and do not revile him.”¹⁴² In addition, in several hadiths, he instructed everyone to refrain from mentioning any negative information about the deceased.¹⁴³

Sharia protects the deceased's information in four ways. First, the person who is going to wash the deceased's body has to meet certain qualifications. For example, the jurists emphasize that the washer has to be a trustworthy person who can be trusted to conceal any uncovered information about the dead body. Further, the washer has to be the same sex as the deceased person; some scholars have made an exception for the spouse.¹⁴⁴ Even if the washer is the same sex as the deceased person, he or she is not permitted to reveal the private parts.¹⁴⁵

¹⁴¹ Alshech, *supra* note 53 at 90.

¹⁴² Sunan Abi Dawud· Book 43, Hadith 127 (Chapter: Regarding the prohibition of speaking ill about the dead).

¹⁴³ Do not abuse the dead because they have attained that which they had forwarded (i.e., their deeds, good or bad)." Al-Bukhari, Book 18, Hadith 54. Also, The Prophet (PBUH) said: Make a mention of the virtues of your dead and refrain from (mentioning) their evils."

¹⁴⁴ Kamali, *supra* note 76 at,220-221.

¹⁴⁵ *Id.*; (what is the private parts), Abu Rafi` Aslam, the freed slave of the Prophet (PBUH) reported: the Prophet (PBUH) said, "He who washes a dead body and conceals what he notices of physical defects, he will be forgiven forty times." Alhakim, Book 7, Hadith 35.

Second, if the washer comes across unusual physical features of the deceased's body, he or she has to conceal whatever he or she witnesses. Ibn Qudama expressed concern that the corpse might have natural defects or might even be marked or altered in a way that would garner disapproval, such as an uncircumcised penis, that, if revealed to others, might damage the deceased's reputation.¹⁴⁶

Third, people, in general, are not allowed to reveal any damaging information about the deceased. Most of the hadiths, as mentioned earlier, direct the public to not share any information that might tarnish the deceased's name.

Fourth, the family members of the deceased have the right to sue anyone who discloses damaging information or secrets regarding the deceased; the person may be punished for this act, or the family can demand financial compensation if they have suffered injury or loss as a result.¹⁴⁷ For example, most of the jurists agreed that if a deceased person is slanderously accused of committing adultery, his or her heirs have the right to demand that the accuser be punished.¹⁴⁸

These four precautions clarify that Sharia protects a deceased person's information from being revealed because such a disclosure of negative information would damage the reputation of the deceased and may cause the deceased person's family to suffer social consequences as well.¹⁴⁹

In fact, most of the prophetic instructions regarding matters such as this focus on damaging information that might harm someone's reputation rather than the secrecy of the information. In other words, sharing negative information about someone else whether this

¹⁴⁶ Alshech, *supra* note 53 at 95.

¹⁴⁷ 10 Ibn Qudamah, *supra* note 65, at 221.

¹⁴⁸ Idris, *supra* note 139 at 156.

¹⁴⁹ Alshech, *supra* note 53 at 96.

information is a private or not is central to this matter and to these rules. Thus, these rules cannot be applied when someone releases non-damaging private information such as a Social Security Number. However, since most confidential information falls under the category of damaging information, these rules can be valuable in that they can serve to protect individuals' privacy.

- **Keeping others' confidential information (*kitman alsir*)**

The second principle that serves to protect people's personal information under the Sharia is the mandate not to disclose any matter a person wishes to conceal from others. Unlike the previous principle, which focuses on damaging information, this principle is wider in scope and aims to protect whatever a person wishes to keep from others. As rightly observed by Alshech, the broader vision was mostly supported and developed by the Islamic scholars from the ninth to the tenth centuries.¹⁵⁰ Explaining the criteria that have been adopted in Sharia to determine the situations in which concealment must be maintained is important for understanding this principle.

The first criterion focuses on the nature of the communication. A leading prophetic hadith explains how Sharia recognizes the personal expectation in defining what information should be protected. Jabir bin Abdullah narrated that the Prophet (PBUH) said, " When a man says something and he looks around, it is an amanah (trust)".¹⁵¹

It is worthy of note that the Prophet was concerned neither with the actual matter discussed by the conversing parties nor with the place in which the conversation took place. Rather, the hadith focuses on the personal belief of the individual. According to Abo-Yala, it is inappropriate to sit between two people while they seem to be talking in a secretive manner, even

¹⁵⁰ Alshech, *supra* note 53 at 98. I believe that this view was also there at the time of The Prophet, showing later.

¹⁵¹ Sunan Abi Dawud, Book 43, Hadith 96, Chapter: Transmitting what others have said.

if they are talking in a public place.¹⁵² The core of this hadith is the personal belief of that person as he or she communicates with the others.

Furthermore, per the hadith, the speaker's act of looking around while talking is sufficient enough to put the listener in the position to refrain from disclosing the information shared during conversation. Al-Mubarakpuri comments on this hadith by stating, "If a man happens to speak to another and he turns around to check if there is anyone around, this talk is considered an amanah (trust). Thus, it is prescribed (la yajoz) to betray the trust by revealing the conversation to others." Ibn Raslan explains that the action of turning around shows the intention of the person to conceal the conversation from others, which is the same as if the person said, "this is a secret, do not tell anyone, or it is a trust."¹⁵³ These scholars recognized the implied action of the person and considered such an action sufficient to result in the same obligation as an explicit agreement. A question might arise, however: Can the person who disclosed a secret be held liable? According to Alhmim, Sharia requires that the two parties must come into an agreement in order for the person who discloses a secret to be held liable.¹⁵⁴ The next section will discuss in detail the related punishments and the compensations.

Another criterion that Sharia uses to distinguish between private and non-private matters is the nature of the relationships in which these matters are disclosed. Researchers who study this issue, based on Islamic jurisprudence, frequently suggest two different types of relationships: professional and non-professional.¹⁵⁵

¹⁵² Abe al-Layth al-Samarqanda asserts that listening stealthily to two people who confer privately [in the public sphere] is inappropriate. Al-Sarakhsa labels such an act as a moral theft. Alshech, *Supra* note 53 at 100.

¹⁵³ Awn al-abd, hadith 4868 at 2240.

¹⁵⁴ See note 79 Alhamim, *supra* note 5 at 304.

¹⁵⁵ Idris, *supra* note 139 (concealing the secret in Sharia Islamic jurisprudence).

- **Professional relationships**

There is no direct text from the Quran or Sunnah governing professional relations with regard to information privacy. Nevertheless, Islamic scholars have developed rules based on a general prophetic hadith that holds that anyone whose counsel is sought is responsible for concealing the matter.¹⁵⁶ The ruling of the hadith was extended by analogy to consultant physicians, lawyers, and bank accountants who are entrusted with their clients' personal information.¹⁵⁷ They are under duty, therefore, not to reveal such information. Classical Islamic scholars, such as Ibn al-hajj, al-Shayzari, and Ibn Bassam, state that the physician is required to protect his patients' secrets and not to disclose to anybody what patients reveal to him.¹⁵⁸ In his book about the medical profession (ayoun alanba fi tbkat alatba), Ibn Abi Usaibia states, "Anything I see or hear during a patient treatment and patients do not usually disclose to the public; I do not reveal it."¹⁵⁹ In addition, Ibn Hubal noted that, before seeing patients, every physician must take an oath to keep patients' secrets.¹⁶⁰

Alshech states that Muslim Scholars were aware that personal matters, such as those having to do with one's body and information about one's lifestyle, in the context of physician-patient relations, are usually disclosed under the pressure of necessity.¹⁶¹ An ill person must share some private information so that the doctor can diagnose his condition accurately and prescribe an appropriate treatment. Thus, Muslim scholars prohibit physicians from disclosing anything they discover as a result of their physician-patient relations.

¹⁵⁶ The Prophet (PBUH) said: "The one whose counsel is solicited is the bearer of *amana*." Sunan Abi Dawud, Book 43, Hadith 356.

¹⁵⁷ Kamali, *supra* note 76 at 216.

¹⁵⁸ 9 AL-SARAKHSI, AL-MABSUT 142 (1993); 4 IBN AL-HAJJ, AL-MADKHAL 35 (1986); and IBN BASSAM, NIHAYAT AL-RUTBAH 109 (2003).

¹⁵⁹ IBN ABI USAIBIA, OYOUN ALANBA FI TBAQAT ALATBA 45 (2001).

¹⁶⁰ IBN HUBAL, MUKTARAT ALTIB 4 (2005)

¹⁶¹ Alshech, *supra* note 53 at 11.

Since the Sharia does not provide any details about what kind of information must be concealed in the context of each type of professional relationship, most of the Muslim countries have developed their own laws that protect personal information based on the nature of the profession such as those related to medicine, banking, and the law. The next chapter will discuss these laws in the context of Saudi Arabia.

- **Non-professional relationships**¹⁶²

Sharia goes beyond prescribing confidentiality in the context of professional relations to include some non-professional relations. For example, the marriage in Islam creates a sacred bond between a husband and a wife that must be honored and protected. Thus, Sharia strictly instructs a husband or a wife to conceal any confidential information about their partner. Revealing confidential information is a breach of a trust created by the marital bond. This is upheld in the hadith, as Abu Sa'id Al-Khudri reported that the Prophet (PBUH) said, "The evilest of the people to Allah on the Day of Resurrection will be the man who consorts with his wife and then publicizes her secret."¹⁶³

This hadith forbids the disclosure of marital secrets by either spouse, practically concerning conjugal relations.¹⁶⁴ Islamic scholars, such as Ibn Abd al-Barr and Ibn Qudama, emphasize this meaning by prohibiting a husband or a wife "[to] discuss [with others] issues related to their marital relations." Because the nature of marriage requires the couple to reveal their bodies and many others secrets, jurists understand that this is a relationship in which private matters are exposed somewhat involuntarily. Therefore, Sharia establishes rules to ensure that the couple does not reveal to others what they have learned about each other's body, habits, etc.

¹⁶² Alshech, *supra* note 53 at 101; Kamali, *supra* note 76 at 217.

¹⁶³ Muslim, Book 2, Hadith 5.

¹⁶⁴ Kamali, *supra* note 76 at 218.

Moreover, confidentiality in the context of a husband-wife relationship appears repetitively when jurists discuss the obligation of a husband to offer his wife a suitable dwelling (maskan) in which to live. Per Islamic law, a husband is required to provide a private residence for his wife as a means of maintaining the confidentiality of their relationship. The only exception occurs when the wife agrees to share the house with someone else such as the husband's mother, father, or sister.¹⁶⁵ Family members other than the husband are entirely deprived of access to information or matters that a wife wishes to conceal. 'Illish states, "[The wife] has the right to refuse to live with any of [the husband's] relatives because she might be harmed when they discover anything she desires to hide from them, even if there is no proof of existing harm."¹⁶⁶ Ibn Rushd further notes that such cohabitation may harm the wife since "[the parents and the other wife's children] become aware of her [private] affairs or anything else she would like to keep hidden from them" (i.e., not only her marital relations).¹⁶⁷

It is critical to note that the jurists who consider these matters and who have put into place constraints do not require that the disclosure of information result in harm or damage. Rather, they recognize the nature of the husband-wife relationship and, therefore, have established restrictions in order to protect the private information of the wife and the stability of the household. Finally, I could not find among the legal sources I consulted discussion regarding the prescription of confidentiality in relations that are neither professional nor marital in nature.

¹⁶⁵ The scholars discuss the condition of living in the same house with a private place. For example, if the husband and his wife live in the same house with the husband's parents but they have a separate unit (room, bathroom, and kitchen). 6 SHAMS AL-DIN, NEHAYAT ALMOHTAJ 382 (1984).

¹⁶⁶ The majority of jurists from the different school that it is not permissible for the husband to force his wife to live in a house with his parents or any other relatives without her approval. He [the husband] has to provide a proper dwelling for the wife alone. 4 MOHAMMAD 'ILLISH, MANH ALGALIL FI MOKTASAR ALKHALIL 395 (1984)

¹⁶⁷ 5 IBN RUSHD, AL-BAYAN WA AL-TAHSIL 450 (1988).

❖ Penalties/ punishment

Punishment in Sharia law depends on the enormity of the crime. First, *Al-hudud* mandated and fixed punishments for particular crimes listed and regulated by the Quran or Sunnah.¹⁶⁸ Second, retaliation (*qasas*) and compensation (*diya*) are also fixed punishments granted for the victims of specific crimes.¹⁶⁹ That is, the victim has the right to pardon the wrongdoer in these crimes.¹⁷⁰ Third, discretionary punishments (*tazir*) are the punishments that are left to the judge to determine based on the particular facts and circumstances of each case. Some scholars state that the *tazir* punishments cannot exceed the *hudud* penalties and should not be predetermined.¹⁷¹

As noted previously, several principles in Sharia are designed to protect the privacy of individuals without specifying certain punishments for each violation of these principles.¹⁷² Hence, the punishments related to violations of privacy principles in Sharia law are *tazir*.

Unlike the *hudud* or *qasas*, the judge, when handing down *tazir* punishment, has the discretion to decide the proper punishment for the wrongdoer in each case. The punishments might vary from a mere reprimand to imprisonment, financial sanctions, or dismissal from his or her job, depending on the facts.¹⁷³

¹⁶⁸ These crimes ranged from moral to monetary and homicidal: adultery, unfounded accusation of adultery, drinking alcohol, highway robbery, and some forms of theft.

¹⁶⁹ When a person is murdered, suffers bodily injury or suffers property damage. TAHIR WASTI, THE APPLICATION OF ISLAMIC CRIMINAL LAW IN PAKISTAN: SHARIA IN PRACTICE (2008).

¹⁷⁰ Whereas the *hudud* no one can pardon the wrongdoer.

¹⁷¹ Hallaq, *supra* note 15 at 165.

¹⁷² In fact, even the Hadith, which allowed the residents to poke the peeper's eye without holding him responsible, did not stipulate the punishment for the crime. Instead, the hadith deprived the peeper of pursuing his right in *qasas* if his eye was poked and preserved the resident right to sue the peeper.

¹⁷³ Imposing financial sanctions is a debatable issue between the scholars. The majority of the four Islamic schools disapprove any financial penalties under *tazir*. However, the judges and the legislators in Saudi Arabia along with most of the modern Islamic countries apply financial penalties as one of the *tazir* punishment. See 10 Ibn Qudamah, *supra* note 65.

A remaining fundamental question has to do with whether the victim of a violation of one of the Sharia privacy principles has the right to demand compensations for his or her personal damages. In Sharia law, the answer to this question depends on the kind of harm the victim has suffered. Sharia scholars have divided personal damages into two types: material damages and moral damages

➤ **Material harm**

Azhily defines material harm as "any damage that harms a person's money or body."¹⁷⁴ With regard to physical bodily injuries, Sharia scholars agree that the victim has the right to demand retaliation (qasas), a certain amount of monetary compensation (dyah), or monetary compensation estimated by the judge according to *ursh* rules depending on which part of parts of a person's body has been injured and how serious the injury is.¹⁷⁵ In spite of their agreement regarding the main principal, Sharia scholars still debate a victim's eligibility for monetary compensation when the harm suffered is indirect. For instance, if the victim's injury case is the result of a disability, can the person demand compensation for the costs of living with a disability? This disagreement has important implications for Saudi judges who tend to award only direct, tangible damages. Since physical bodily injuries do not usually result from violations of privacy, this dissertation will not go into detail regarding the rules associated with bodily injury compensations.

In terms of harm that affects a person's finances, Sharia scholars have looked to the Islamic principle "There should be neither harming [darar] nor reciprocating harm [diraar]" to

¹⁷⁴WAHBAH AZHILY, ALTAEWID EAN ALDARAR MIN ALMADIN ALMUMATIL [COMPENSATION FOR DAMAGE FROM THE DEFAULT DEBTOR] 12 (2001).

¹⁷⁵ The majority of the Sharia scholars require the damages to be actual and direct. MOHAMMAH BUSAQ, ALTAEWID EAN ALDARAR FI ALFAQIH AL'IISLAMII [COMPENSATION FOR DAMAGE IN ISLAMIC JURISPRUDENCE] 39 (1998).

come to the agreement that a harmed person has the right to demand monetary compensation for the amount he or she lost as a result of the defendant's misconduct. The Saudi courts and laws are full of examples of monetary compensation for financial harm.

➤ **Moral harm**

Moral harm is defined as the non-physical damage that affects a person's feelings, emotions, reputation, dignity, or honor.¹⁷⁶ These damages generally result from defamation, slander, or the disclosure private information. Studying the controversial issues surrounding moral harm in Sharia is a vital part of this dissertation since privacy violations result primarily in moral harms. Moreover, although it is important to compensate the victim of moral damage to protect the privacy right of individuals, this issue (i.e., compensating the victim of moral damage) remains unclear and is still debated among Sharia scholars. This ambiguity has impacted the Saudis courts, as this dissertation will show in the third chapter.

It is worthwhile to identify and assess the issues in Sharia law regarding probable punishments and compensations as they relate to moral harm. First, the majority of Sharia scholars agree that a person who causes another person to suffer moral harm might be subject to different types of punishments. These punishments could be mandated and fixed (hudod), such as in case of an unfounded accusation of adultery where the accuser will receive 80 lashes,¹⁷⁷ or they could be discretionary punishments (tazir). Discretionary punishments, as mentioned previously, could be imprisonment or financial sanctions that go to the government rather than to

¹⁷⁶ ALI ALKHAFEEF, ALDAMAN FI ALFAQIH AL'IISLAMII [LIABILITY IN ISLAMIC JURISPRUDENCE] 38 (2000).

¹⁷⁷ "And those who accuse chaste women and then do not produce four witnesses - lash them with eighty lashes and do not accept from them testimony ever after. And those are the defiantly disobedient" Quran, surah AL Noor (24:4).

the defendant. Further, it is undisputed that if the moral harm results in financial harm, the defendant has the right to demand monetary compensation for the financial damage he or she has suffered. For example, a morally harmed person who lost his or her job because of an unfounded accusation that had a negative effect on his or her reputation will have the right to demand monetary compensation for his or her loss. Third, a controversial question exists regarding whether the morally harmed person has the right to demand monetary compensation for purely moral harm.

It is critical to note here that none of the classical jurists have mentioned this issue in their books.¹⁷⁸ Nevertheless, contemporary Sharia scholars have discussed and debated this question in depth. The majority of these scholars, as well as the International Islamic Fiqh Academy, believe that Sharia does not provide for monetary compensation for the victim of moral damages.¹⁷⁹ The primary reason for their refusal, according to Al-Zarqa, is that it is challenging to find a fair and consistent manner through which to estimate an appropriate amount of compensation, as Sharia maintains that damages and compensation should adhere to the principle of equivalence.¹⁸⁰ Moreover, in the Quran, the only punishment for false accusation of adultery is 80 lashes with no monetary compensation.¹⁸¹

However, some Sharia scholars, as well as most of the current legal systems in the Islamic countries, allow for monetary compensation as a result of moral damage.¹⁸² Regarding

¹⁷⁸ 13 THE KUWAITI ENCYCLOPEDIA OF ISLAMIC JURISPRUDENCE 40 (2005)

¹⁷⁹ Busaq states that the majority opinion is to not allow monetary compensation for the victim of moral damages. Busaq, *supra* note 175 at 34. Also, Alkhafef, Alsarqa, and Alsanhory agree with the majority. Alkhafef, *supra* note 176 at 46.

¹⁸⁰ *Id.* at 45.

¹⁸¹ MUSTAFA ALZARQA, ALFIEL ALDAAR WA ALDUMAN [HARMFUL ACTION AND LIABILITY IN ISLAMIC JURISPRUDENCE] 19 (1988).

¹⁸² Alzhily, Abdulsami, and Aljirid believe that Sharia law allows monetary compensation for the victim of moral damages. WAHBAH AZHILY, *NAZARIAT ALDAMAN* [THEORY OF LIABILITY IN SHARIA] 25 (2012); OSAMAH ABDULSAMI, ALTAEWID EAN ALDARAR AL'ADBII DIRASATAN TATBIQIATAN FI ALFAQIH ALI

the general principle, Abdulsami states, "There should be neither harming nor reciprocating harm," and the harm here includes moral harm. As a result of such a prohibition against any kind of harm, monetary compensation is one method, per Sharia, by which the materially and morally harmed may be compensated. For instances, the third caliph sentenced a man who beat another man until he urinated as a result of his intense fear to compensate the defendant with a third of dyah. Ibn Qudamah stated, in *AlMogani*, that the dyah in Sharia is compensation for a person who lost a part of his or her body or who was subjected to mutilation of the body, whereas the compensation in Othman's division was for the fear since there was no injury.¹⁸³

The next chapter will discuss the ongoing argument regarding monetary compensation for moral damages in Saudi Arabia, where some courts have chosen to reward the morally harmed person with financial compensation, and others continue to refuse to financially compensate the morally harmed person. This inconsistency directly affects the information privacy system. The third chapter will explain this in greater details, and the fourth chapter will recommend solutions.

❖ Conclusion

When Islam emerged, principles and rules were introduced which significantly increased the protection of individuals' privacy. These include the following: 1) preventing any intrusion, regardless of how the information is obtained, to individuals' homes, papers or confidential conversations; 2) imposing a new set of rules that regulate how to seek permission before entering someone's house or coming between two people who appear to be having a confidential conversation in a public place; 3) maintaining the confidentiality of the individual's private

¹⁸³ ISLAMII [COMPENSATION FOR MORAL DAMAGE APPLIED STUDY IN ISLAMIC JURISPRUDENCE] 210 (2014); K. ALJIRID, ALTAEWID EAN ALDARAR ALMADIYI WALMAENAWII WATATBIQATI ALQADAYIYA [COMPENSATION FOR PHYSICAL AND MORAL DAMAGE AND ITS JUDICIAL APPLICATIONS] 437 (2011).

¹⁸³ 13 Ibn Qudamah, *supra* note 65, at 12.

information by criminalizing any disclosure of any information that may lead to harm of another person, and the order to conceal others' private information, especially confidential information that appears through a certain necessity such as a physician-patient relationship or a husband-wife relationship. These principles were able to provide a high level of protection regarding the privacy of individuals at that time. The generality and the reliance on the general custom made these principles applicable in different places and times.

Today, however, thanks to the technological revolution, the amount of personal information available has dramatically increased, and sharing information has become much easier, which poses a risk to individual privacy. The Sharia principles and rules that protect information privacy need to be further developed to provide individuals with the same level of privacy protection as the principles meant to give and did give before the digital era. These enhancements might result from either more detailed laws or judges who can improve the principles through cases. The next chapter will focus on examining the information privacy system in Saudi Arabia and the level of protection provided via its current laws and judges.

Chapter 2: Information Privacy in Saudi Laws

❖ Introduction

The legal system in Saudi Arabia relies on both Islamic jurisprudence and written laws. The previous chapter presented how a number of principles of Sharia serve to protect individuals' privacy. This chapter provides an overview of the legal protection of individuals' privacy achieved via Saudi written laws. The importance of this chapter lies in the paucity of studies that review all laws intended to protect individuals' information privacy in Saudi Arabia. The published legal studies in the field of privacy law in Saudi Arabia discuss primarily the protection of privacy provided by a particular law¹⁸⁴ or one aspect of privacy such as compensation associated with one's privacy being violated or violating privacy through espionage.¹⁸⁵ What follows is discussion regarding how current Saudi laws provide for legal protection of individuals' right to privacy, especially the privacy of digital information. The subsequent chapter explains why the current level of information privacy protection offered by both Islamic jurisprudence and written legislations is inadequate.

➤ The Legal System in Saudi Arabia

▪ Introduction to the Basic Law of Saudi Arabia

The Basic Law is a constitution-like charter promulgated in 1992. It contains rights and obligations; state authorities; financial affairs; and audit institutions. Article 1 of The Basic Law of the Kingdom states, "The Kingdom of Saudi Arabia is a sovereign Arab Islamic State. Its religion is Islam. Its constitution is Almighty God's Book, The Holy Qur'an, and the Sunnah, or traditions, of the Prophet 'PBUH.' Arabic is the language of the Kingdom. The City of Riyadh is

¹⁸⁴ See Alsolami, *supra* note 6.

¹⁸⁵ See Al-Qahtani, *supra* note 7. See Also Alshahri, *supra* note 7.

the capital."¹⁸⁶ Article 7 confirms, "The government in the Kingdom of Saudi Arabia derives its authority from the Book of God and the Sunnah of the Prophet 'PBUH,' which are the ultimate sources of reference for this Law and the other laws of the State."¹⁸⁷ Thus, laws and regulations must be consistent with the Quran and Sunnah.

Moreover, it stipulates economic principles, rights, and obligations that obligate the state to protect human rights in conformity with Sharia principles, maintain the state's public funds, guarantee the inviolability of private homes and communications, and safeguard private property and people's freedom from unlawful arrest and punishment.

Additionally, the Basic law of Governance states that the authorities of the state include judicial authority, executive authority, and regulatory authority. The three powers cooperate with each other, and the King is the point of reverence for all of these authorities.¹⁸⁸ There is no separation of power, especially between the executive and legislative branches.

- **State Authorities**
 - **Executive Branch**

The executive branch consists of the King, the Council of Ministers, local government, ministries, and other independent public agencies. The King has full authority over the executive branch in his capacity as King and Prime Minister. According to article 55 of the Basic Law, the King carries out the national policy in accordance with the provisions of Islam.¹⁸⁹ The King oversees the implementation of Sharia, the nation's system of government, the statutory laws, and the state's general policies.¹⁹⁰

¹⁸⁶ The Basic Law of Governance, SA §1. (1992).

¹⁸⁷ The Basic Law of Governance, SA §7. (1992).

¹⁸⁸ The Basic Law of Governance, SA §44. (1992).

¹⁸⁹ The Basic Law of Governance, SA §55. (1992).

¹⁹⁰ The Basic Law of Governance, SA §55. (1992).

The Council of Ministers, which is led by the King as the prime minister, is the direct executive authority. The Council consists of the Prime Minister, the Crown Prince, and Cabinet ministers. According to Article 19 of the Law of the Council of Ministers, the Council is empowered to determine the internal, external, financial economic, educational, and defense policies.¹⁹¹ The Council has the final authority in the financial and administrative affairs of all ministries and other government agencies.¹⁹² The Council also plays the primary role in the legislative branch.

- **The Legislative (Regulatory) Branch**¹⁹³

The legislative branch is shared among the King, the Council of Ministers, and the Consultative Council (Majlis Al-Shura). The King fills the central rule-making role. The Basic Law describes the King as the ultimate authority over and above all State authorities, including the legislative authority.¹⁹⁴ Per Royal Order, he is authorized, as Head of State and the prime minister, to enact, repeal, or amend any laws and regulations. Additionally, the King has the final decision regarding any drafted law, enactment of international treaties, agreements, regulations, and concessions, after these items are first reviewed by the Kingdom's legislative bodies (i.e., the Council of Ministers and the Shura Council).

The Council of Ministers undertakes legislative functions in addition to serving in an

¹⁹¹ The Law of Council Ministers SA § 19 (1993)

¹⁹² The Law of Council Ministers SA § 19 (1993)

¹⁹³ Under Sharia, which forms the basis of the legal system in Saudi Arabia, God is the sole lawmaker. So, the word “legislator” which implies secular law is not used in Saudi Arabia. Instead, The Basic Law uses the term “regulatory authority” to refer to the legislative authority in Saudi Arabia, which has the authority to enact statutory laws and regulations and approve international treaties, agreements, regulations, and concessions. Abdullah Ansary, *A Brief Overview of the Saudi Arabian Legal System*, GLOBAL LAW AND JUSTICE, at

http://www.nyulawglobal.org/globalex/Saudi_Arabia1.html#_Toc424144441 (last visited Nov. 13, 2018).

¹⁹⁴ The Basic Law of Governance, SA §44. (1992). See David J. Karl, *Islamic Law in Saudi Arabia: What Foreign Attorney's Should Know*, 25 Geo. Wash. J. Int'l L. & Econ. 141 (1991).

executive capacity. Each minister is allowed to propose a bill or regulation related to his ministry. The proposed bill or regulation will be on the table so that the council's members may vote on it. If the majority of the council votes in favor the new law, the King will enact the law by the King's decree.¹⁹⁵ Once the King decrees the new law, it must be published in the government gazette, "the Umm al-Qura newspaper," to be effective.¹⁹⁶ Finally, the related ministry or department has to issue any necessary policies and procedures to carry out the approved rules.

The legislative branch is also shared by the Al-Shura Council, which was established pursuant to the Basic Law of 1992. The Shura Council is an institution intended to provide consultation to the King, exercise oversight functions, and allow citizens to participate directly in the administration and planning of national policies.¹⁹⁷ The King appoints all the 150 members of The Council of Al-Shura.¹⁹⁸ The members are professors, experts in business, economy, education, military and law fields, and scholars.¹⁹⁹ The proposed laws and regulations will be subject to discussion and vote by the Al-Shura's members before they are sent to the Council of the Ministers for voting and approval.²⁰⁰ Finally, the King will either adopt or reject the proposed law. It is worth noting that the legislative authority must take care to ensure that the legislation does not conflict with the Quran or valid Sunnah, which serve as Saudi Arabia's constitution.²⁰¹

¹⁹⁵ *Id.* at 142.

¹⁹⁶ *Id.*

¹⁹⁷ The Law of Council Al-Shura, SA § 15 (1992)

¹⁹⁸ The Law of Council Al-Shura, SA § 3 (1992)

¹⁹⁹ The Law of Council Al-Shura, SA § 3 (1992)

²⁰⁰ The Law of Council Al-Shura, SA § 16 (1992)

²⁰¹ The Law of Council Al-Shura, SA § 2 (1992)

- **The Judicial Branch**²⁰²

The Saudi judicial system is divided primarily into two judicial bodies: Sharia courts and the Board of Grievances (an administrative judicial body). Each of these judicial bodies has jurisdiction over cases brought before it. Sharia courts are the general courts that have jurisdiction in all claims and cases that do not fall under the jurisdiction of other courts or juridical committees. The Board of Grievances, on the other hand, has jurisdiction over all claims that involve government bodies as a party. Additionally, several juridical committees have jurisdiction over specific claims²⁰³; these include the Committee for Banking Disputes, the Committee for the Settlement of Labor Disputes, the Committee for the Settlement of Insurance Disputes, and the Committee for the Settlement of Securities' Disputes. These committees were established to solve some issues that the Sharia courts were unable to address quickly and consistently whether because of heavy caseloads or the subject matter of the case.²⁰⁴

- ◆ **Sharia Courts**

In 2007, King Abdullah issued a Royal decree approving significant amendments to the structure of the judicial system. First, Sharia courts are divided into three categories: the High Court at the top of the judicial hierarchy, the Courts of Appeal in the middle, and the First-Degree Courts at the lowest level.

²⁰² The explanation of the judicial system in Saudi Arabia in this chapter is according to the Law of the Judiciary 2007, Royal Decree No. M/78, art. 5, (19/9/1428H, Oct. 1, 2007), O.G. Umm al-Qura No. 4170 (30/9/1428H, Oct. 12, 2007).

²⁰³ A Royal Decree under which the committee was constituted will determine what kind of claims the committee has jurisdiction to hear.

²⁰⁴ Some of these committees were established because the judges in the Sharia courts will not decide on the case that might contradict the Sharia law. For example, in the banking disputes, the Sharia courts would exclude any elements or claims involve Riba or "banking interest" from the case, but the banks wanted the hearing to cover all the elements even the banking interest "Riba." See ABDULRAHMAN AL-MASNAD, UNCLAIMED MONEY IN SAUDI BANKS 27(2016). Available at <https://www.repository.law.indiana.edu/etd/30/> (last visited Nov. 13, 2018).

The High Court plays several legislative, consultative, and judicial roles. The court ensures the implementation of Sharia law and regulation enacted by the King.²⁰⁵ Further, the High Court reviews the decisions of the Courts of Appeal. It is mandatory to "review sentences involving death, amputation, or stoning."²⁰⁶ In these specific cases, the High Court acts as a court of subject-matter/trial court. In other matters, the High Court still has the right to review the decisions of the Courts of Appeal whenever the issue is a question of law or a question of procedure - not question of fact with one exception.²⁰⁷

The Law of the Judiciary of 2007 established the Courts of Appeal as a new level of litigation in the Sharia courts. The Law forms one or more court of appeal in each of the Kingdom's provinces.²⁰⁸ Each court contains five specialized circuits, including criminal, personal status suits, labor suits, commercial suits, and civil suits circuits.²⁰⁹ The ruling of the Court of Appeal is binding, unless the judgment includes "death, amputation, or stoning"; then the Supreme Court must review it.²¹⁰

The lowest level of the Sharia courts is the First-Degree Court. The First-Degree Courts are being spread throughout Saudi Arabia's provinces and cities in accordance with the needs of a given region.²¹¹ This level includes several specialized courts, which are a summary court, personal status court, labor court, a commercial court, and general courts.²¹² It also has specialized circuits, including enforcement, approval and traffic circuits.²¹³ The general court has

²⁰⁵ The Law of the Judiciary, SA §11. (2007).

²⁰⁶ *Id.*

²⁰⁷ *Id.*

²⁰⁸ The Law of the Judiciary, SA §15. (2007).

²⁰⁹ Each circuit is comprised of three judges, except for the criminal circuit, which reviews decisions involving major offenses. *See* The Law of the Judiciary (2007), SA §16. (2007).

²¹⁰ The Law of the Judiciary (2007), SA §11. (2007).

²¹¹ The Law of the Judiciary (2007), SA §18. (2007).

²¹² The Law of the Judiciary (2007), SA §19. (2007).

²¹³ The Law of the Judiciary (2007), SA §19 &20. (2007).

jurisdiction over all disputes that do not fall under another court's jurisdiction.²¹⁴ The summary court has jurisdiction over retaliation "Qisas" and "Hudud" cases, "Tazir" cases, and Juvenile cases. It might worth mentioning that the Minister of Justice established a specialized criminal court in the city of Riyadh to assume jurisdiction over cases involving terrorism, national security, and other related offenses.²¹⁵ The decisions made by these courts are subject to be reviewed by the Court of Appeal.

◆ The Board of Grievances

The Board of Grievances is the second type of judiciary system in Saudi Arabia. It is an independent administrative, judicial commission directly associated with the King. The Board of Grievances has jurisdiction over any case against the government.²¹⁶ The Board, which comprises of three levels of courts: The Administrative Court, the Administrative Court of Appeals, and the Supreme Administrative Court, has a similar structure as the Sharia Court. It is worth mentioning that some of the juridical principles of the Board of Grievances, such as those regarding compensation for moral damage, might contradict with the principles of Sharia courts.²¹⁷

❖ Privacy in Saudi Arabia's Legislation

Many provisions relating to the sanctity and safety of individuals' personal data are spread out over many legislative instruments. This chapter examines the level of protection

²¹⁴ The Law of the Judiciary (2007), SA §23. (2007).

²¹⁵ The Minister of Justice issued order No. 1422 of January 28, 2009, based on Supreme Judicial Council resolution No. 4/69 of January 6, 2009. The Law of Terrorism Crimes and Financing, Royal Decree No. M/16, art. 8, (24/2/1435 H, Dec. 27. 2013), O.G. Umm al-Qura, (30/3/1435, Jan. 31, 2014), defines the terrorist crimes and other related offenses that threaten the national security.

²¹⁶ Until the new judiciary system of 2007 fully applied, The Board of Grievances still has jurisdiction over some of the commercial cases.

²¹⁷ The subsequent chapter explains in detail the issue of having a different point of view regarding the compensation for moral damage between the Board and Sharia courts and the effect of that disagreement on the privacy right.

offered by these laws, especially given the digital context, by providing an overview of each law and discussing how effectively it can be used to protect individuals' information privacy.

➤ **The Basic Law of Governance of 1992**

The Basic Law, which is similar to other countries' constitutions in terms of what it includes, recognizes the privacy of individuals as an essential right in a number of ways. First, the Basic Law declares that the state protects individuals' rights in accordance with Sharia law. This includes the privacy of individuals as one of the rights highly protected by Sharia law, as described in the previous chapter. Second, the Basic Law contains two articles that explicitly state that the privacy of individuals must be protected. Article 37 of the Basic Law places emphasis on the sanctity of the home; it reads, "The home is sacrosanct and shall not be entered without the permission of the owner or be searched except in cases specified by statutes."

Moreover, article 40 of the Basic Law recognizes the importance of protecting personal communications in the digital age. It explicitly states, "Telegraphic, postal, telephone, and other means of communications shall be safeguarded. They cannot be confiscated, delayed, read or listened to except in cases defined by statutes."²¹⁸ The significance of this article lies in the fact that it includes all means of communications and does not specify only some means.²¹⁹ This makes the article applicable to modern means of communication such as email and new chat

²¹⁸ The Basic Law of Governance, SA §40. (1992).

²¹⁹ It is important to mention that the power of the administrative court to review the executive actions is limited. According to Al-jarbou, the power of the Board of Grievances differs under the administrative liability, which is considered to be a violation of a specific right of the plaintiff, and the administrative legality, which is considered to be a violation of the rule of law. The role of Board's juridical to review of administrative actions under legality principles is the maintenance of the rule of law. Thus, the Board's power is limited to annul the challenged administrative action. On the other hand, the role of the Board's juridical review of administrative actions under liability principles is "corrective justice". The Board has full power to annul and amend the administrative actions and to compensate for damages. For more information about the Board of Grievances and its power of juridical review see Judicial Review of Administrative Actions Under Saudi Law. AYOUB A. AL-JARBOU, JUDICIAL REVIEW OF ADMINISTRATIVE ACTIONS UNDER THE SAUDI LAW 221-22 (2011).

applications.²²⁰

➤ Law of Criminal Procedures (2013)

The Law of Criminal Procedure emphasizes the privacy protection granted by the Basic Law of Governance, and it does so via greater detail. In article 40, the Law of Criminal Procedures extends the protection given to homes to include offices and vehicles, and it defines “homes” as “any place enclosed within barriers or intended to be used as a dwelling.”²²¹ More importantly, article 56 of the law proscribes any surveillance of mail, cable, telephone, or other means of communication except with a valid warrant.²²² The Executive Regulation of the Law of Criminal Procedure states that the protection granted by article 56 of the law includes any modern means of private communications.²²³

The articles protecting privacy in the Basic Law of Governance and the Law of Criminal Procedures focus on safeguarding the sanctity of individuals’ homes and bodies as well as their private communications rather than their personal information in general. Nonetheless, some

²²⁰ Msfer Al-Qahtani, *Hmayat Alhayat Alkhasat lil'iinsan Watatyabaqatiha Alqadayiya (Alasrar- Almrslat-altqnyat Almeasr) Dirasat Mqarn* [Protecting the Privacy of Humans and its applications courts: (Secrets, Communication, New Technologies): A Comparative Study.] 68 (2014) (unpublished Ph.D. dissertation, Imam Mohamad Bin Saud University) (on file Imam Mohamad Bin Saud University Library) available at <http://www.alukah.net/web/triqi/0/31722/>.

²²¹ Chapter IV: Search of Persons and Dwellings, article 41 states “The privacy of persons, their dwellings, offices, and vehicles shall be protected. The privacy of a person protects his body, clothes, property, and belongings. The privacy of a dwelling covers any fenced area or any other place enclosed within barriers or intended to be used as a dwelling”. Article 57 explains the legal procedures to disclose personal mail, paper, or to record telephone conversation, “The Director of the Bureau of Investigation and Prosecution may issue an order authorizing seizure of mail, publications, and parcels and surveillance and recording of telephone conversations, if such procedure is deemed useful in determining the truth related to a crime that has actually been committed. Such order shall state the reasons thereof and shall be for a period not exceeding ten days renewable according to the requirements of the investigation.” Law of Criminal Procedures, SA §41, 57(2013).

²²² Chapter V: Seizure of Mail and Surveillance of Conversations. Article 56: “Mail, cables, telephone conversations and other means of communication shall be inviolable and, as such, shall not be perused or surveilled except pursuant to an order stating the reasons thereof and for a limited period as herein provided for.” Law of Criminal Procedures, SA §56(2013).

²²³ The Executive Regulation of the Law of Criminal Procedure, SA §37. (2015).

commentators tend to extend the protection of articles 41, 42, 45, and 48 from the Law of Criminal Procedures to include personal information in their cell phone devices.²²⁴

For example, the Awareness Committee at Mohammad Bin Saud University asked students who broke some of the university's rules to hand over their phones so that the phones could be inspected. The students were told that refusing to hand over their phones could result in the students' dismissal, which would prevent them from continuing their studies or completing their exams. The story became public when the dean, Moodi Al Dubayan, defended the action of the committee to Saudi television channel Rotana Khaleejia.²²⁵ Many legal commentators who argued against the university action built their arguments on the protection of the person's belongings under articles 41 and 56 of the Law of Criminal Procedures.²²⁶

However, the language of article 41 defines the boundaries of "home" but does not define what a person's "belongings" might include; neither the Executive Regulation of the Law of Criminal Procedure nor any published cases define this either.²²⁷ Further, article 56 prohibits the violation of any private communications. The protection is limited to the communications such that it does not directly protect all information or all data on a given device. Thus, these articles

²²⁴ Article 48: "The criminal investigation officer may not open sealed or closed documents found in the dwelling of the accused. A statement to this effect shall be entered into the record and be submitted to the competent Investigator." Law of Criminal Procedures, SA §48, 57(2013).

²²⁵ *Dean Wades into Controversy Over Cell Phone Search*, GULF NEWS, Oct. 9, 2017, available at <http://gulfnews.com/news/gulf/saudi-arabia/dean-wades-into-controversy-over-cell-phone-search-1.2102675>.

²²⁶ *Taftish Jwwalat Alttalibat Mukhalafat Watajawuz Ealaa "alkhususia" Wala Ytmu 'iilaa bi'amr Alniyaba [Inspecting students' mobile phones is a violation of the "privacy" if it is not ordered by the prosecution]*, SABQ ONLINE NEWSPAPER, Oct. 8, 2017, at <https://sabq.org/ZsfDkc>.

²²⁷ Article 41: "A criminal investigation officer may not enter or search any inhabited place except in the cases provided for in the laws, pursuant to a search warrant specifying the reasons for the search, issued by the Bureau of Investigation and Prosecution. However, other dwellings may be searched under a search warrant, specifying the reasons, issued by the Investigator. If the proprietor or the occupant of a dwelling refuses to allow the criminal investigation officer free access or resists such entry, he may use all lawful means, as may be required in the circumstances, to enter that dwelling. A dwelling may be entered in case of a request for help from within, or in case of a demolition, drowning, fire, or the like, or in hot pursuit of a perpetrator." Law of Criminal Procedures, SA §41, 57(2013).

are ambiguous and do not necessarily protect a phone from being arbitrary searched. In fact, in 2013, the head of Committee for the Promotion of Virtue and the Prevention of Vice issued an administrative circular prohibiting the Commission's members from searching people's phones. The administrative circular based the prohibition on the violation of general principles of Sharia law, provisions of the Law of Criminal Procedures, without specifying which articles, and another administrative circular issued by the Minister of Interior. The administrative circular issued by the Minister of Interior prohibits searching phones except in cases of flagrant delicto.²²⁸

In summary, the Law of Criminal Procedures provides considerable protection to the privacy of homes and private communications against official governments; however, the law does not provide the same level of protection to personal information in general. The language is too broad, and it is difficult to interpret the intent of the legislator because the decisions of courts are not binding on other courts and are rarely published.

➤ **The Anti-Cyber Crime Law (2007)²²⁹**

The Anti-Cybercrime Law comprises sixteen articles that outline or identify the key definitions, intended goals, cybercrimes, sentences, and fines. This law aims to combat cybercrimes by identifying such crimes and determining their punishments to ensure information security and to protect rights regarding the legitimate use of computers and information networks, public interests, morals, common value, and national economy.²³⁰ Even though the Anti-Cybercrime law might be considered relatively recent in terms of its inception and implementation, the goals of this law, as stated in the second article, do not explicitly address the

²²⁸ The administrative circular Number: 1/5/2/50025/2 on 10/1/2006

²²⁹ The Anti-Cyber Crime Law issued by Royal Decree Number M/17 on 26th March 2007.

²³⁰ The Anti-Cyber Crime Law, SA §2. (2007).

protection of privacy as a primary concern of the law.²³¹ However, practically, this law, directly and indirectly, protects individuals' privacy via several provisions, which will be the focus of this section.

▪ **Definitions**

In the first article, the law defines the most important terms used in this law; some of these terms include “information system,” “information network,” “data,” “computer,” “computer programs,” and “unauthorized access.”

Unlike the Law of Criminal Procedures, the privacy protection offered by the Anti-Cybercrime Law is not limited to individuals against official governments. The law defines “person” as any natural or corporate person whether public or private.²³² Anyone who violates the Anti-Cybercrime Law will face criminal charges and probable civil suits; yet, according to article 8 of the law, an aggravating circumstance in which a judge is required to sentence the offender to not less than half the maximum punishment is if the offender holds a public office and the crime perpetrated relates to this office, or if he or she perpetrates the crime using the power or influence of his or her public position.²³³

The law provides broad definitions of “computer” and “unauthorized access.” A computer, per the law, is any electric device whether movable or fixed, wired or wireless, which is equipped with a system to process, store, transmit, receive, or browse data, and performs specific functions according to programs and commands. Further, the law defines “unauthorized access” as deliberate, unauthorized access by any person to computers, websites,²³⁴ information

²³¹ The Anti-Cyber Crime Law, SA §2. (2007).

²³² The Anti-Cyber Crime Law, SA §1/1 (2007).

²³³ The Anti-Cyber Crime Law, SA §8 (2007).

²³⁴ "Website: a site providing data on the information network through specific Uniform Resource Locator (URL)"

systems,²³⁵ or computer networks.²³⁶

The law does not require the computers, websites, information systems, or computer networks to be protected by passwords or any means of protection. In fact, unauthorized access is punishable even if the owner or the legitimate user of a computer, system, or network has not taken sufficient care to protect his or her computer, system, or network. In addition, illegal access includes any access to another's computer without the consent of the legitimate user of that computer or system, no matter whether the access direct or remote.²³⁷ The unauthorized access of another's computer, information system, or site constitutes a crime even if the perpetrator does not have a specific intent to harm the present.²³⁸

Finally, the law defines "data" as information, commands, messages, voices, or images, which are prepared or have been prepared for use in a computer. This includes data that can be saved, processed, transmitted, or constructed by computers, such as numbers, letters, and codes, and "reception" is illegal viewing or obtaining of data.

▪ **Types of crimes covered by this law according to punishment**

This law criminalizes many illegal actions that involve the use of computers or computer networks; the criminal acts include blackmail,²³⁹ defamation,²⁴⁰ infliction of damage upon others,²⁴¹ unlawful acquisition of movable property or bonds, identity theft,²⁴² illegally accessing bank or credit data or data pertaining to ownership of securities with the intention of obtaining

²³⁵ "Information system: a set of programs and devices designed for managing and processing data, including computers."

²³⁶ "Information network: an interconnection of more than one computer or information system to obtain and exchange data."

²³⁷ Alshahri, *supra* note 6 at 58-59.

²³⁸ *Id.*

²³⁹ The Anti-Cyber Crime Law, SA §3/2 (2007).

²⁴⁰ The Anti-Cyber Crime Law, SA §3/5 (2007).

²⁴¹ The Anti-Cyber Crime Law, SA §1/1 (2007).

²⁴² The Anti-Cyber Crime Law, SA §4/1 (2007).

data, information funds to services offered,²⁴³ human trafficking,²⁴⁴ and the preparation, publication, and promotion of material for terrorism,²⁴⁵ pornographic,²⁴⁶ gambling,²⁴⁷ and psychotropic drugs sites.²⁴⁸ As the scope of this dissertation involves the study of privacy protection, the discussion that follows will have to do with provisions that are directly related to the privacy of individuals.

- **Article 3**

In article 3,²⁴⁹ the law states that any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding one year and a fine not exceeding five hundred thousand riyals, or either punishment:

- 1- Spying on, interception or reception of data transmitted through an information network or computer without lawful authorization.
- 2- Unauthorized access to a computer with the intention to threaten or blackmail any person.
- 3- Unlawful access to a website, or hacking a website with the intention to change its design, destroy or modify it, or occupy its URL.
- 4- Invasion of privacy through the misuse of a camera-equipped mobile phone and the like.
- 5- Defamation and inflation of damage upon others through the use of various information technological devices.

²⁴³ The Anti-Cyber Crime Law, SA §4/2 (2007).

²⁴⁴ The Anti-Cyber Crime Law, SA §6/2 (2007).

²⁴⁵ The Anti-Cyber Crime Law, SA §7/1 (2007).

²⁴⁶ The Anti-Cyber Crime Law, SA §6/3 (2007).

²⁴⁷ The Anti-Cyber Crime Law, SA §6/3 (2007).

²⁴⁸ The Anti-Cyber Crime Law, SA §6/4 (2007).

²⁴⁹ The Anti-Cyber Crime Law, SA §3 (2007).

Eight out of sixteen cases that have been officially published by the Ministry of Justice as cyber crimes were based on article 3 of The Anti-Cyber Crime Law.²⁵⁰ This article safeguards the privacy of individuals in several ways.

The first paragraph prohibits any kind of spying or interception of transmitted data, no matter whether the data was secured properly or not as long as there is no legitimate authority. Focusing on the authorization rather than the level of security protects the information of the average person whose network and computer are usually insufficiently protected.

The second paragraph criminalizes anyone who accesses a computer with the intention to blackmail or threaten another person. Generally, unauthorized access with such intention will target private or valuable information; therefore, the law criminalizes mere illegal entry. The punishment, according to this paragraph, does not substitute the punishments decided by the sharia courts based on tazir rules for a person who commits the crime of threatening or blackmailing another person; rather, it is an additional punishment for unlawfully accessing a computer combined with the intention to blackmail or threaten.²⁵¹ This paragraph indirectly protects the individual's valuable and sensitive information from being remotely or directly accessed without his or her permission. However, the law here does not protect the information; it protects the computer. Thus, if a blackmailer takes possession of sensitive information without accessing a computer, the law will not be applicable.

Similarly, the fifth paragraph protects private information indirectly by generally criminalizing the use of any technological devices for purposes of defamation or inflation of

²⁵⁰ Case number: 3451637 Date: 1/3/1434 H, Case number: 34206789 Date: 6/5/1434 H, Case number: 34226363 Date: 28/5/1434 H, Case number: 32164059 Date: 26/6/1434 H, Case number: 34277055 Date: 32/7/1434 H, Case number: 3521012 Date: 1435H, Case number: 35165932 Date: 1435 H

²⁵¹ Case number: 34226363 Date: 28/5/1434 H, Case number: 32164059 Date: 26/6/1434 H, Case number: 34277055 Date: 32/7/1434 H, Case number: 35165932 Date: 1435 H

damage upon others. Because technology can facilitate the possibility of defamation and damage upon others remotely and makes it difficult for authorities to identify the perpetrator or the accused, legislators increased the penalty for the use of technology to defame and harm others. Disclosing private information through the use of technological devices can serve as one means of defaming and inflating damage upon others.²⁵²

More importantly and directly, the fourth paragraph protects privacy by imposing penalties on anyone who misuses a mobile phone with a camera so as to violate the privacy of others. The language here is broad.²⁵³ The law states, "Invasion of privacy through the misuse of a camera-equipped mobile phone and the like," without any further explanation, which might result in unanswered questions. What constitutes an invasion of privacy? Is the legal provision exclusive to the violation of privacy through a "mobile phone"? What about other devices such as cameras, recording devices, and GPS devices? Further, today, phones are not unlike computers. In other words, phones can be used to facilitate or complete many functions or processes. For example, someone can take a picture with his or her phone and store this picture and send it to another person who can then post it at one of his or her social media accounts. In this scenario, the phone was used to produce, store, send, and post the picture, so what of these actions constitutes "misuse"? Unfortunately, the answer can only be extracted from a limited number of published cases.

In one of the published cases,²⁵⁴ the judge applied this paragraph when the defendant took a picture of an 11-year-old girl in a store and sent it to another person. The judge decided that the action was an invasion of privacy even though the picture was taken in a public place.

²⁵² Case number: 34206789 Date: 6/5/1434 H

²⁵³ ASHRAF HILAL, VIOLATING THE RIGHT TO PRIVACY ACCORDING TO "ANTI-CYBERCRIMES LAW IN SAUDI ARABIA" 157 (2015).

²⁵⁴ Case number: 35165932. Date: 1435 H. Page: 295

The judge merely recounted the decision without explaining the reasons why this action was a violation of privacy. The Court of Appeal upheld the judge's ruling. With the scarcity of similar published cases that explain the terms of the paragraph, the judge is left with considerable discretionary power, and this might vary from case to case.

- **Article 4**

In article 4, the law states that any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding two million riyals, or either punishment: “Illegally accessing bank or credit data, or data pertaining to ownership of securities with the intention of obtaining data, information, funds, or services offered.”

With stricter penalties, this paragraph offers protection of people’s banking and credit information. Rather than focusing on the crime of stealing the money through illegal access to banking or credit data, the law protects the information by criminalizing mere "illegal access." It is considered a full-fledged crime even if the accused is unable to obtain money as a result of illegally accessed data.²⁵⁵ However, to apply this law, the defendant has to use a computer to access the data.²⁵⁶

- **Article 5**

In article 5, the law states that any person who commits one of the following cyber crimes shall be subject to imprisonments for a period not exceeding four years and a fine not exceeding three million riyals, or either punishment: “Unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter, or redistribute private data”; “Cause the

²⁵⁵ Hilal, *supra* note 253 at 131.

²⁵⁶ *Id.*

information network to halt or breakdown, or destroy, delete, leak, or alter existing or stored programs or data.”

These two paragraphs serve as information security protection, which, in many cases, overlap with privacy protection. Additionally, the legislator specifically mentions “private data” in the first paragraph of article 5. No further clarification has been given about what data is considered private.²⁵⁷

- **Article 6**

In article 6, the law states that any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding five years and a fine not exceeding three million riyals, or either punishment: “Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through an information network or computer.”²⁵⁸

The court widely used this paragraph to incriminate the accuser under the Anti-Cybercrime law. Not surprisingly, eight out of sixteen published cases relied on article 6. The fact that the legislator used very general language, and that very strict sentences may result from violations of the law, prompt the Attorney General to find the law satisfactory and make it hard for judges to deny the law. This paragraph addressed a range of cyber crimes, including crimes related to blackmail, and the storage of pornographic videos and private pictures of others. Because of the vague language used, article 6 might be the most useful legal instrument currently in Saudi Arabia aimed at ensuring individual’s privacy and protecting them against cybercrimes that might violate their privacy.

²⁵⁷ For more explanation about the elements of this crime see Hilal, *supra* note 253 at 148.

²⁵⁸ The Anti-Cyber Crime Law, SA §4(2007).

- **Articles 9 & 10**

The law extends the stated punishments to any person who attempts to commit any of the crimes described in this law.²⁵⁹ Likewise, the punishments associated with this law can be applied to anyone who incites, assists, or collaborates with others to commit any of the crimes described in this law.²⁶⁰

- **Article 15**

According to article 15, the Public Prosecution shall be responsible for the investigation and prosecution of the crimes stipulated in this law.²⁶¹ Nevertheless, it is important to mention that article 16 of Law of Criminal Procedures allows the harmed person, under certain conditions, the right to initiate criminal proceedings against the accused, even if the Public Prosecution does not conduct any legal action, and permits the court to reach a judgment that effectively compensates him or her for the damage caused by the crime.²⁶² Thus, a claim of privacy violation, in accordance with the rules of the Anti-Cybercrimes Law, entitles the claimant to the right to compensation for damages caused by the violation of the law.²⁶³ Privacy violation causes moral, as well as, material damages. Although article 16 of Law of Criminal Procedures does not specify the type of damage to be compensated, material or moral damage,

²⁵⁹ “Any person who attempts to commit any of the crimes stipulated in this law shall be subject to punishment not exceeding half the maximum punishment designated for said crime” The Anti-Cyber Crime Law, SA §10 (2007).

²⁶⁰ “Any person who incites, assists or collaborates with others to commit any of the crimes stipulated in this law shall be subject to punishment not exceeding the maximum punishment designated for such crimes, if the crimes committed as result of said incitement, assistance or collaboration, and he shall be subject to punishment not exceeding half the maximum punishment designated, if the intended crimes are not committed” The Anti-Cyber Crime Law, SA §9 (2007).

²⁶¹ The Anti-Cyber Crime Law, SA §15(2007).

²⁶² “The victim (or representative of his heirs – in case of death – may initiate a criminal action with respect to all cases involving a private right and shall pursue such case or action before the competent court. In such a case, the court shall summon the public prosecutor.” Law of Criminal procedures, SA §16 (2013)

²⁶³ Al-Qahtani, *supra* note 7 at 184.

the judicial system in Saudi Arabia is still not clear about the eligibility of the victim for compensation as result of moral damage; this will be discussed more in depth later in subsequent chapter.

In conclusion, the Anti-Cybercrimes Law in Saudi Arabia protects, directly and indirectly, individuals' privacy. However, using terms that are not easily defined, such as “public order,” “religious values,” “public morals,” and “privacy,” in an incriminating article may cause many issues regarding legal adaptation.²⁶⁴ The line between a criminal and non-criminal act is fuzzy, and this raises the possibility that people will inadvertently commit criminal acts. Moreover, prosecutors may find it difficult to define the criminal line and present evidence.²⁶⁵ In the end, with no case law system, each judge will have to define these unclear terms and apply the law.²⁶⁶ To define these terms, each judge will have to go back to the principles of Sharia law and general custom, which are too general and not easily applies to today’s issues, as explained in the previous chapter and establish his own definition and borders regarding privacy.

Furthermore, the Anti-Cybercrimes Law is not proactive, as it protects only privacy that has been violated through a criminal act. The provisions of this law operate only after the cybercrime has occurred. The law does not outline any positive steps that can be taken to prevent privacy violations from happening. For instance, a network or a computer is a subject of the

²⁶⁴ Asel Aljaid, *Altashhir Wahuriyat Alraay Kamaqhumun Qanuniyn [Defamation and freedom of opinion as legal concepts]*, ALWATAN NEWSPAPER, Jan. 30, 2018, at <http://www.alwatan.com.sa/Articles/Detail.aspx?ArticleId=36289>.

²⁶⁵ Asel Aljaid, *Nizam Aljarayim Almaelumatia Yueani min Daef Alsiyaghat Wasueubat Altakyif Alqanunii [The Anti-cybercrimes Law suffers from poor drafting and difficulty in legal adaptation]*, ALMADINAH, Nov. 25, 2013, available at, <https://www.al-madina.com/article/268337/>.

²⁶⁶ For more explanation about the issues of not having defined terms and the difficulties faced by the judge to carry out her work to the fullest extent, see generally Marwan Alrowqi, *Alqasad Aljinayiyu fi Aljarayim Almaelumatia [Criminal intent in cybercrime]* (2011) (unpublished thesis, Naif Arab University for Security Sciences) (on file with Naif Arab University for Security Sciences Library), available at <https://repository.nauss.edu.sa/handle/123456789/52106>.

protection of this law even if the user or owner does not take any precaution steps. Further, to prove that a crime has occurred, it is necessary to prove its material and intentional elements. The requirements regarding a crime's elements limit the protection provided by law. Many privacy violations result from the misuse of personal data that has been legally obtained.

➤ **E-Transaction Law and its Executive Regulation** ²⁶⁷

E-transaction law aims to control, regulate, and provide a legal framework for electronic transactions and signatures.²⁶⁸ As is the case of the Anti-Cybercrimes Law, E-transaction law does not explicitly indicate that information privacy is one of the objectives of the law.²⁶⁹ E-transaction law does not define "personal information" or provide special rules for public and private institutions that deal with private information. Instead, the law established several rules for dealing with any electronic data, which includes more than just the personal data, and electronic records in general to maintain the credibility and integrity of electronic transactions.²⁷⁰ Ultimately, regulating electronic transactions provides some indirect protection for personal data.

Before digging into the rules of the E-transaction law and its executive regulation, it is critical to explain the scope of this law. Article 3 of the law states that the law applies to all E-transactions²⁷¹ and signatures, excluding the following:

- 1- Transactions related to personal status law

²⁶⁷ The Royal Decree No (M/18) dated 26 March 2007 approved the E-transactions Law. Article 30 of the E-Transactions Law, the Ministry of Communications and Information Technology issued an executive regulation for e-transactions under the Council of Ministers Decision No 2 dated 3/18/2008.

²⁶⁸ E-Transactions Law, SA §2 (2007).

²⁶⁹ E-Transactions Law, SA §2 (2007).

²⁷⁰ The law defines electronic data as "data with electronic features in the form of texts, codes, images, graphics, sounds, or any other electronic form, either collective or separate." E-Transactions Law, SA §1/11(2007). Also, electronic records were defined as "data generated, communicated, received, or stored, by electronic means, and retrievable in perceivable form." E-Transactions Law, SA §1/13 (2007).

²⁷¹ The law defines electronic transactions as "Any exchange, communication, contracting or other procedure, performed or executed, wholly or partially, by electronic means." E-Transactions Law, SA §1/10(2007).

2- Issuance of deeds of legal actions related to real property²⁷²

Thus, the law applies to any natural or corporate person, whether public or private.

▪ **Storing Data**

The law and its executive regulations stipulate several rules for storing electronic data. First, electronic data must be stored in compliance with the requirements of any relevant laws, regulations, or procedures that apply to the storage of traditional data (i.e., non-electronic data).²⁷³ In other words, laws and regulations governing the storage of traditional data will be stretched to include electronic data as well. There is no clarification, however, about which laws and regulations have been extended.

Second, electronic data shall be stored correctly and in their natural and original forms without modification.²⁷⁴ This article is meant to ensure the validity of the retained data. The law and its executive regulations do not specify how the data should be verified, or even grant the data subject the right to verify or correct the stored data.

Third, the executive regulation stipulates that if any laws or regulations specify time or duration of data retention, data has to be kept safe for that duration.²⁷⁵ Here, the regulation serves to ensure that the data related to electronic transactions²⁷⁶ is stored for at least the amount of time specified via the related laws. In another words, the executive regulation of E-transaction law does not require anyone who retains electronic data to delete the data after a certain period. In fact, the focus was to ensure that the data is stored for a minimum amount of time. Nevertheless, the executive regulation emphasizes that the parties to the E-transaction must comply with their

²⁷² E-Transactions Law, SA §3(2007).

²⁷³ The Executive Regulations of the E-Transactions Law, SA §2/1 (2008).

²⁷⁴ The Executive Regulation of the E-Transactions Law, SA §2/2 (2008).

²⁷⁵ The Executive Regulation of the E-Transactions Law, SA §4/1 & §5/4 (2008).

²⁷⁶ “Electronic Transactions: Any exchange, communication, contracting or other procedure, performed or executed, wholly or partially, by electronic means.” E-Transactions Law, SA §1/10 (2007).

bilateral agreements regarding how to store the data and protect related parties' privacy, as long as their agreement does not conflict with relevant laws.²⁷⁷

Fourth, anyone who is responsible for storing electronic data or records must follow precise and reliable rules and standards to ensure the safety of the stored records against unauthorized access or unauthorized modification. The rules shall include the process of application, examination, and disaster recovery plans.²⁷⁸ The legislator does not impose certain standards to safeguard the stored data. Instead, the executive regulations allow the public and the private institutions the freedom to set their own security standards without any further instructions. Therefore, the security standards may vary from one institution to another, especially given the absence of sanctions for not applying a reasonable standard of security.

▪ Accessing the Data

The executive regulation has established some requirements for accessing the stored data. First, any institution that retains electronic data has to limit the power of accessing the data and records to certain employees based on necessity.²⁷⁹ Additionally, the institution has to bind all workers to its standards for protecting the privacy of data and records.²⁸⁰

Second, any institution that retains electronic records is obliged to apply the appropriate technical solutions to register all cases in which such electronic records are accessed or changed.²⁸¹ The law and its executive regulation do not provide any further instructions regarding how to maintain a record of all data access cases or how long the access records should be maintained.

²⁷⁷ The Executive Regulation of the E-Transactions Law, SA §3/13 (2008).

²⁷⁸ The Executive Regulation of the E-Transactions Law, SA §5/3 (2008).

²⁷⁹ The Executive Regulation of the E-Transactions Law, SA §6/2 (2008).

²⁸⁰ The Executive Regulation of the E-Transactions Law, SA §6/2 (2008).

²⁸¹ The Executive Regulation of the E-Transactions Law, SA §6/3 (2008).

Third, the parties of the transaction and the legally authorized entities have the right to access the related data.²⁸² Conversely, the institution that maintains the records is not entitled to enable third parties to access the records without previous agreements between or among the parties.²⁸³

▪ **Consent**

With regard to consent, the law requires implicit or explicit permission before electronic transactions may be completed. Article 4 of the law states, “Nothing in this Law shall compel any person to use electronic transactions without his implicit or explicit consent.”²⁸⁴ The law excludes government agencies; when government agencies serve as the relevant parties, then explicit approval is required before an electronic transaction may take place.²⁸⁵ No further requirements have been stated with regard to the language of the request for consent or about the right to withdraw consent.

▪ **Penalties**

The law in article 23 lists ten offenses punishable by a fine not exceeding five million riyals or imprisonment for a period not exceeding five years, or both penalties.²⁸⁶ The offenses punishable by law have to do with authentication services, data or electronic signature forgery.²⁸⁷ None of these offenses are related to protecting data privacy. Moreover, the Communications and Information Technology Commission, in cooperation and coordination with competent authorities, is in charge of recording and inspecting violations listed in article 23.²⁸⁸

²⁸² The Executive Regulation of the E-Transactions Law, SA §6/4 (2008).

²⁸³ The Executive Regulation of the E-Transactions Law, SA §6/4 (2008).

²⁸⁴ E-Transactions Law, SA §4/1 (2007).

²⁸⁵ E-Transactions Law, SA §4/2 (2007).

²⁸⁶ E-Transactions Law, SA §23&24 (2007).

²⁸⁷ E-Transactions Law, SA §23 (2007).

²⁸⁸ E-Transactions Law, SA §25 (2007).

It is vital to note here that the Commission’s authority to inspect is limited to the listed offenses. The provisions related to protecting privacy are not within the jurisdiction of the Commission, which means that the Commission is not entitled to inspect for such violations. For example, if an institution does not comply with any of the requirements related to data storage, the harmed person must find the violation and approach the court to seek compensation. According to article 27, “Any person incurring damage – due to violations set forth in this Law or failure to comply with any controls or obligations provided for therein – shall reserve the right to claim damages before the competent judicial authority.”²⁸⁹

In conclusion, E-transaction law and its executive regulation provide some legal protection regarding electronic data and records in general by instructing the entities that maintains electronic data and records to limit the power to access the data to the fewest employees possible, to keep the records of every access case, to acquire consent before storing the data, and to prohibit third-party access without the consent of the parties subject to the transaction or legal authorization.

However, the law and the executive regulation clearly do not aim to protect individuals’ personal data. The legal protection provided by the law and its executive regulation to individuals’ personal data is still insufficient and indefinite. For example, the law lacks a clear definition regarding what constitutes personal data and sensitive data. The law does not distinguish between the types of data and thus treats all types equally. With the absence of these essential definitions, it is difficult to provide individuals with adequate protection of their private data. Either the level of protection extended to all data needs to be raised, and this would prove unreasonable for most institutions, or the level of protection extended to all data, including

²⁸⁹ E-Transactions Law, SA §27 (2007).

personal data as it relates to E-transactions law, needs to be lessened.

Moreover, regarding the violations of the rules, there are no specific penalties for those who violate the rules aimed at protecting data. In addition, the inspection of such violations is not under the jurisdiction of the Commission. Thus, practically, individuals whose personal data has been compromised are responsible for discovering the privacy violations, proving that the violations occurred, and demanding compensation at the court. Finally, since most of the privacy violations cause moral damages and general courts in Saudi Arabia are still inconsistent in terms of the right to compensation for moral damage, taking such a case to the general Sharia courts puts one at risk of not receiving any compensation.

➤ **The Telecommunications Law and its Executive Regulation²⁹⁰**

Unlike the Anti-Cybercrimes and E-transactions Laws, protecting individuals, personal information is one of the declared goals of the Telecommunications Law. Under the “objectives” stated in article 3 of the Telecom law, The legislature explicitly declares that one of the main goals of the law is “to safeguard the public interest and the user interest as well as maintain the confidentiality and security of telecommunications information”²⁹¹ The existence of this objective is reflected in several provisions of the law and its executive regulation.

▪ **Article 9 of The Telecommunications Law**

Article 9 of the law emphasizes the confidentiality and inviolability of telephone calls and information transmitted or received through the public telecommunications network and prohibits any kind of intrusions without legal ground.²⁹² Essentially, the article confirms the

²⁹⁰ The Royal Decree No (M/12) dated 3 June 2001 approved the Telecommunications Law. The Ministry of Communications and Information Technology issued an Executive Regulation for the Telecommunications Law under the Council of Ministers Decision No. (11) dated 27 July 2002.

²⁹¹ Telecommunications Law, SA §3/8 (2001).

²⁹² “Article Nine: The privacy and confidentiality of telephone calls and information transmitted or received through public telecommunications networks shall be maintained. Disclosing, listening or

provisions of Article 40 of the Basic Law of Governance. It is important to recognize that this article is concerned with the calls and information transmitted through the communications companies, not consumers' personal information being held by the communications companies.

- **The Executive Regulation of The Telecommunications Law**
 - **Article 56 (Confidentiality of User Information)**

The executive regulation provides greater and unprecedented protection of the privacy of individuals' data. First, in article 56, the legislators hold the service providers responsible for maintaining users' private information.²⁹³ The article also clarifies the mechanism of objection or complaint if the service providers breach their responsibility.²⁹⁴

Second, article 56 identifies the personal information that the company is entitled to disclose; the article reads, "A service provider shall not disclose information other than the user's name, address and listed telephone number to anyone without the user's written consent or unless disclosure is required or permitted by the Commission²⁹⁵ or by law to another legally authorized public authority."²⁹⁶ Here, the legislator prohibits the service providers from disclosing any information about a user except the user's name, address, or listed telephone number without prior permission from the user or the existence of other legal grounds. However, the legislator allows service providers to disclose the user's name, address, and telephone number without stating limitations. According to this paragraph, service providers have the right to disclose users' listed information without any legal obstacles. The legislator did not link this

recording the same is not permitted, except for the cases stipulated by the relevant Acts." Telecommunications Law, SA §3/8 (2001).

²⁹³ "A service provider's liability for disclosure of user information contrary to this Article shall be determined in accordance with Chapter 13 of this Bylaw." Executive Regulation for the Telecommunications Law SA §56/2 (2002).

²⁹⁴ I will explain later the process of the complaint.

²⁹⁵ The Communications and Information Technology Commission.

²⁹⁶ The Executive Regulation for the Telecommunications Law SA §56/1 (2002).

right to having a specific and reasonable reason for disclosing such information. This might be the primary reason behind the widespread reception of many solicitation calls in Saudi Arabia.²⁹⁷

Third, article 56 grants users the right to access and modify their information; the article reads, “Upon request, users are permitted to inspect any service provider’s records regarding their service. Users shall have the right to require that any user information contained in their records that they can demonstrate is incorrect, be corrected or removed.”²⁹⁸ The paragraph does not mention who bears the costs of copying of the information or the period during which the service providers must deliver the information to the user.

Fourth, the legislation states that billing information shall not be used for any purpose other than billing, and the information must be retained for a given period of time according to Saudi law.²⁹⁹ The legislator did not specify what constitutes billing information or what specific laws determine for how long the billing information must be retained.

Finally, the legislator states again that concerned government agencies are allowed to access confidential information relating to a user in accordance with the laws of Saudi Arabia.³⁰⁰

- **Article 57 (Confidentiality of User Communications)**

Article 57 not only ensures the confidentiality of the users’ communications in accordance with article 9 of the law, but it also holds the service providers responsible for taking

²⁹⁷ Abdullah Alrowqi, *Almutajarat Bibayanat aleumala' Zahirat Muzeajat fi Alsewdyt Tantashir dun Quayud [Trading customers' information: An alarming phenomenon in Saudi Arabia spread without restrictions]*, ALEQTISADYAH, Sep. 14, 2017, available at http://www.aleqt.com/2017/09/14/article_1251356.html.

²⁹⁸ The Executive Regulation for the Telecommunications Law SA §56/3 (2002)

²⁹⁹ “All user-specific information, and in particular billing-related information, shall be retained by a service provider only for billing purposes and retained only for so long as it is required by the laws of the Kingdom.” The Executive Regulation for the Telecommunications Law SA §56/4 (2002)

³⁰⁰ “Nothing in this Bylaw shall be interpreted to prohibit or infringe upon the rights of concerned government agencies to exercise their rights to access otherwise confidential information relating to a user. Such access shall be made in accordance with the laws of the Kingdom.”

reasonable steps to maintain the confidentiality of users' communications. The article reads as follows, "Service providers shall take all reasonable steps to ensure the confidentiality of user communications in accordance with Article Nine of the Act."³⁰¹ Additionally, the article specifies the procedural steps necessary to trace and locate a source of harassing, offensive, or illegal calls.³⁰²

- **Article 58 (Protection of Personal Information)**

Before discussing the rules of article 58, it might be worth mentioning that the term "personal information," which the legislation behind this article included in the article, has never before or since been used in Saudi law. Unfortunately, no definition or explanation has been provided to identify precisely what constitutes personal information; yet, article 58 contains several vital rules aimed at protecting individuals' information.

First, service providers are responsible not only for user communications but also for any user information of which the providers or their agents are in control.³⁰³ This paragraph places more responsibility on the service providers and their agents. The subsequent paragraphs within the same article offer greater explanation regarding the nature of the service providers'

³⁰¹ The Executive Regulation for the Telecommunications Law SA §57/1 (2002)

³⁰² "For the purposes of tracing and locating a source of harassing, offensive or illegal calls;

a) A user may request that the Commission authorize a service provider to monitor calls to the user's telephone;

b) The Commission or other duly authorized authority in the Kingdom may direct a service provider to monitor calls to and from a user's telephone and the service provider shall comply with any such direction;

c) The service provider shall provide the Commission the information resulting from its monitoring of the user's telephone, including the telephone numbers that are the source of the harassing, offensive, or illegal calls and the dates of occurrence of such calls and their frequency; and

d) The Commission may undertake any appropriate action to protect the public from harassing, offensive or illegal calls in accordance with the Commission statutes, and if necessary refer the matter to the appropriate authorities for further action." The Executive Regulation for the Telecommunications Law SA §57/3 (2002).

³⁰³ "A service provider shall be responsible for user information and user communications in its custody or control and in that of its agents." The Executive Regulation for the Telecommunications Law SA §58/1 (2002).

responsibilities.

Second, the legislation prohibits service providers from disclosing, collecting, maintaining, or using users' personal information except if it is allowed by law or is based on the user's consent as stated in the second paragraph of the article 58, which reads, "A service provider shall operate its telecommunications facilities and telecommunications network with due regard for the privacy of its users. Except as permitted or required by law, or with the consent of the person to whom the personal information relates, a service provider shall not collect, use, maintain or disclose user information or user communications for any purpose."³⁰⁴ This might be the clearest and most detailed legal provision aimed at protecting the personal information of individuals in Saudi Arabia. The legislator here does not instruct service providers to generally protect users' personal information, but it explicitly stipulates that users' personal information shall not be disclosed, collected, maintained, or used unless there is prior permission from the user or the existence of a legal authority.

Third, the legislation continues to elaborate on the nature of the service providers' responsibility to protect users' personal information by prohibiting any collection of users' information before disclosing the purpose of the data collection as stated in the third paragraph, which reads, "The purposes for which user information is collected by a service provider shall be identified at or before collection, and a service provider shall not, subject to this Article, collect, use, maintain or disclose user information for undisclosed purposes."³⁰⁵ Here, the third paragraph is concerned with collecting users' information. The legislation has added a condition beyond obtaining the user's prior permission or a gaining authorization based on a legal provision, and this condition states that the service providers have to disclose the purpose of such collection of

³⁰⁴ The Executive Regulation for the Telecommunications Law SA §58/2 (2002).

³⁰⁵ The Executive Regulation for the Telecommunications Law SA §58/3 (2002).

data and shall not use the information for other purposes. No further instructions are given regarding the validity of the purpose.

Fourth, one of the service providers' responsibilities is to ensure the accuracy of the users' information as stated in the fourth paragraph of the article, which reads, "Service providers shall ensure that users' information is accurate, complete and up to date for the purposes for which it is to be used and that user information and user communications are protected by security safeguards that are appropriate to their sensitivity."³⁰⁶ Notably, the legislator in this paragraph requires that users' information and communications shall be protected according to their sensitivity without describing what constitutes the most sensitive or least sensitive information.

- **Article 59 (Users Complaints)**

Article 59 gives the Communications and Information Technology Commission the authority to handle complaints between users and service providers if the subject matter of the dispute is regarding the service providers' use of the users' confidential information.³⁰⁷ Another distinct feature of this law is that a specialized commission, not a general court, will review the case and decide whether or not the service provider committed a violation.

In conclusion, compared to other Saudi laws related to the protection of individuals' privacy, the telecom law and its executive regulation provide well-defined legal provisions. The law and its executive regulation stipulate that any collection, disclosure, or use of a user's personal information must be based on law or prior permission. Further, the law enables the communications and information technology commission to hear the user's complaint regarding any violation of his or her privacy committed by a service provider. Enabling a specialized body

³⁰⁶ The Executive Regulation for the Telecommunications Law SA §58/4 (2002).

³⁰⁷ The Executive Regulation for the Telecommunications Law SA §59/10 (2002).

to oversee telecom companies' practices, develop relevant laws through regulations, and hear users' complaints helps to ensure greater protection of individuals' rights to privacy.

However, the provisions of the law and its executive regulation are still characterized by generality. For example, the executive regulation requires that service providers shall disclose their purposes before collecting information about individuals.³⁰⁸ The executive regulation, however, does not explain whether or not the service providers must have valid and reasonable purposes.

Further, the executive regulation prohibits any disclosure of any information regarding the user, other than the user's name, address, and telephone number, without the user's permission or a law that permits such disclosure. The legislator did not elaborate regarding to what extent service providers are allowed to disclose a user's name, address, and telephone number. Disclosing such information about an individual might cause a lot of harm to the individual's right to privacy.

Additionally, although the executive regulation requires that service providers shall obtain the user's permission before collecting, disclosing, and using his or her personal information, no further instructions were given regarding the clarity of the language used to request the user's permission. A review of the privacy policy of the three telecommunications companies that operate in Saudi Arabia, which are STC, Mobily, and Zain, indicates that all of the companies offer very brief privacy policies that are lacking in detail.³⁰⁹ The companies tend to use a general language. For example, in Mobily's privacy policy, the company states that it

³⁰⁸ The Executive Regulation for the Telecommunications Law SA §58/3 (2002)

³⁰⁹ STC privacy policy, *available at*

<https://www.stc.com.sa/wps/wcm/connect/english/privacyStatement/Privacy+Statement> ; Mobily privacy policy, *available at* <https://support.mobily.com.sa/privacy?lang=en> ; and Zain privacy policy, *available at* https://www.sa.zain.com/autoforms/portal/site/personal/privacypolicy?AF_language=en.

collects what it referred to as "non-personal information" and might share such information with a third party for marketing, advertising, or other uses. The company's privacy policy is devoid of any definition of what is meant by non-personal information; rather, the policy provided only examples of non-personal information, which included the user's "IP address, cookie information, [the user's] local language, and the page [the user] requested." Lastly, all the three companies state in their privacy policies that they reserve the right change their respective policies anytime, and they made no mention of any intention to notify the user in the event that they do actually change their privacy policies.

➤ **Cloud Computing Regulatory Framework (2018)**

On February 6, 2018, the Communications and Information Technology Commission (CITC) issued the Cloud Computing Regulatory Framework (CCRF).³¹⁰ The CCRF regulates "Cloud Services" in Saudi Arabia, including the rights and obligations of service providers and the cloud consumers such as individuals, government entities, and private companies. In addition to the CCRF, the CITC published the following documents: Guide for Cloud Service Providers; Individual Customers' Guide to Cloud Computing Services; Enterprises' Guide to Cloud Computing Services; and Government Agencies' Guide to Cloud Computing Services.³¹¹ By discussing the CCRF, this dissertation focuses on the provisions that offer protection to individuals' personal information.

▪ **The Scope of the Cloud Computing Regulatory Framework**

³¹⁰ Cloud Computing Regulatory Framework, SA (2018), *available at*

<http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx>.

³¹¹ Communications and Information Technology Commission (CITC), Guide for Cloud Service Providers; Individual Customers' Guide to Cloud Computing Services; Enterprises' Guide to Cloud Computing Services; and Government Agencies' Guide to Cloud Computing Services (Feb. 6, 2018), *available at* <http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx>.

Generally, the CCRF applies when any cloud service is provided to customers who are Saudi residents or who have an address in Saudi Arabia.³¹² The cloud services are defined as any information and communications technology services provided via cloud computing, and these can include the storage, transfer, or processing of customer content.³¹³ Additionally, the CCRF applies when a cloud service provider processes or stores “any Customer Content and Customer Data, permanently or occasionally, in Datacenters or other elements of a Cloud System that are located in the Kingdom.”³¹⁴

▪ **Classification of customers content**

In the CCRF, customers’ contents are subject to different levels of information security, depending on the confidentiality, integrity, and availability as defined in the table below:³¹⁵

Classification of Customer Content by Level of Required Information Security	Categories of Customer Content
Level 1	<ul style="list-style-type: none"> - Non-sensitive Customer Content of individuals or private sector companies not subject to any sector-specific restrictions on the outsourcing of data - Customer Content qualifying for Level 2 or Level 3 treatment, for which the Cloud Customer agrees to Level 1 treatment
Level 2	<ul style="list-style-type: none"> - Sensitive Customer Content of individuals, not subject to any sector-specific restrictions on the outsourcing of data - Sensitive Customer Content of private sector companies or organizations, not subject to any sector-specific restrictions on the outsourcing of data - Non-sensitive Customer Content from public authorities - Customer Content qualifying for Level 1 or Level 3 treatment, for which the Cloud Customer requests Level 2 treatment

³¹² Cloud Computing Regulatory Framework, SA §3.1 (2018).

³¹³ Cloud Computing Regulatory Framework, SA §2.2.1 (2018).

³¹⁴ Cloud Computing Regulatory Framework, SA §3.2 (2018).

³¹⁵ Cloud Computing Regulatory Framework, SA §3.3.1 (2018).

Level 3	<ul style="list-style-type: none"> - Any Customer Content from private sector-regulated industries subject to a level categorization by virtue of sector-specific rules or a decision by a regulatory authority - Sensitive Customer Content from public authorities - Customer Content qualifying for Level 1 or Level 2 treatment, for which the Cloud Customer requests Level 3 treatment
Level 4	<ul style="list-style-type: none"> - Highly sensitive or secret Customer Content belonging to relevant government agencies or institutions

Furthermore, the CCRF places a number of statutory presumptions on how the cloud service providers should classify customer content (unless the cloud customer has requested a specific level of protection). The presumptions are:

- for natural persons with a residence in the Kingdom: Level 1 treatment of Customer Content;
- for private sector legal persons, such as companies, other corporate entities, and associations or organizations incorporated or with a customer address in the Kingdom: Level 2 treatment of Customer Content;
- for any government or state services or agencies: Level 3 treatment of Customer Content; and
- for all other categories: Level 1 treatment of Customer Content.³¹⁶

▪ **Data protection**

The CCRF establishes some rules to protect customer content. First, the CCRF regulates the transfer of customer content outside of Saudi Arabia. For example, the cloud service providers must inform their customers in advance whether their customer content will be permanently or temporarily transferred, stored, or processed outside of Saudi Arabia.³¹⁷ More importantly, the CCRF prohibits any transfer of Level 3 content outside of Saudi Arabia for any

³¹⁶ Cloud Computing Regulatory Framework, SA §3.3.4 (2018).

³¹⁷ Cloud Computing Regulatory Framework, SA §3.3.11 (2018).

reason unless expressly allowed by other laws or regulations of the Kingdom.³¹⁸ Second, the CCRF requires the cloud service providers to notify their consumers and/or the CITC of any security breaches that are likely to affect customer content. For instance, cloud service providers must inform their cloud customers of any security breaches or information leaks.³¹⁹ However, if the security breach or information leak is likely to affect any Level 3 customer content or the data belonging to a significant number of people, the cloud service provider must notify the CITC.³²⁰ Third, the CCRF prohibits cloud service providers from processing any Level 1 or Level 2 customer content unless they have obtained the customers' prior explicit permission (via an 'opt-in' or an 'opt-out' form).³²¹ Lastly, the cloud service providers are obligated to grant the customers "the right and the technical capability to access, verify, correct, or delete their Customer Data."³²²

Notably, the CCRF focuses primarily on protecting Level 3 content, which usually concerns government entities, rather than individuals' content. For example, cloud service providers can transfer their customers' content (Level 1 and Level 2 content) outside of Saudi Arabia without first obtaining customers' permission. The cloud service providers are required only to notify their customers before transferring the data. It might be reasonable to focus on the governmental data, but the government entities would have the upper hand when they sign the

³¹⁸ Cloud Computing Regulatory Framework, SA §3.3.8 (2018). Also, the CCRF prohibits any Level 3 content to be transferred, stored, or processed in any Public Cloud, Community Cloud, or Hybrid Cloud, unless and for as long as they are validly registered with the CITC. Cloud Computing Regulatory Framework, SA §3.3.9 (2018).

³¹⁹ Cloud Computing Regulatory Framework, SA §3.3.12 (2018)

³²⁰ Cloud Computing Regulatory Framework, SA §3.3.13 (2018)

³²¹ Cloud Computing Regulatory Framework, SA §3.4.3.2 (2018)

³²² Cloud Computing Regulatory Framework, SA §3.4.4 (2018)

cloud service contract. Thus, the government entities can include their demands. Individuals, on the other hand, are usually signing adhesion contracts.

Nevertheless, the CCRF is a step in the direction of clearer regulations aimed at protecting personal information by providing individuals with essential privacy rights. The CITC reserves the right to add, clarify, and modify the CCRF.³²³ For instance, the CITC has not yet established specific penalties associated with the violation of the CCRF rules. Instead, the CCRF states, “Any violation of the provisions of this Regulatory Framework shall be subject to the penalties that the Commission may impose under Commission Statutes.”³²⁴ Further, the CCRF does not identify the ways in which the cloud service providers must notify their customers in the event of a security breach.

➤ **Banking Consumer Protection Principles 2013**³²⁵

While article 4 of the Anti-Cybercrime law provides protection against illegal access to banking and credit data, the Saudi Arabian Monetary Agency (SAMA)³²⁶ extended the privacy protection by issuing the Banking Consumer Protection Principles (BCPP). These principles are binding for banks,³²⁷ and they aim to protect financial consumers on several levels such as

³²³ “Complementing this Regulatory Framework through mandatory or voluntary detailed implementation provisions.” Cloud Computing Regulatory Framework, SA §3.10 (2018).

³²⁴ Cloud Computing Regulatory Framework, SA §3.10.1(2018).

³²⁵ The ‘Banking Consumer Protection Principles’ is the guiding document that will support the licensed banking institutions (banks) to deliver the necessary level of fair treatment, honesty, and financial inclusiveness and meet SAMA’s strategic objective for financial consumer protection in the Kingdom of Saudi Arabia. The ‘Banking Consumer Protection Principles’ are issued under powers granted to SAMA under the following legislation and regulation: (a) Charter of the Saudi Arabian Monetary Agency – Article (3d), issued by Royal Decree No. 23. Dated 15/12/1957G. (b) Banking Control Law issued by Royal Decree No. M/5. Dated 12/6/1966G. (c) Ministerial Decree No.3/2149. Dated 22/6/1986G. Banking Consumer Protection Principles SA §4 (2013).

³²⁶ “The Saudi Arabian Monetary Agency (SAMA) is the regulator and supervisor of licensed financial institutions including banks, finance companies, leasing and real estate companies, insurance companies, money exchanger companies and credit information companies in the Kingdom of Saudi Arabia.”

³²⁷ Banking Consumer Protection Principles SA §4/2 (2013).

ensuring fairness and fair treatment, increasing transparency, and protecting consumers' personal information.

Through a number of rules, these principles also offer some protection of customers' personal information. First, article 5 recognizes the adoption of the "G20 High-Level Principles on Financial Consumer Protection."³²⁸ Principle 6, which is entitled "Protection of Privacy," states "Consumers' financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used, and disclosed (especially to third parties)."³²⁹ Further, SAMA, in its Arabic version of the BCPP, adds that banks also have to adhere to all of the listed administrative circulars issued by SAMA regarding matters of privacy.

In addition, SAMA has noted the numbers and dates related to seven administrative circulars regulating how banks shall treat customers' private information. All seven of the administrative circulars were sent to Saudi banks; however, only two of the seven administrative circulars were officially published on SAMA's website.³³⁰ Circular number (14547) served primarily to remind the banks of previously published circulars and to ensure that the banks shall not provide any local or foreign entities (such as international payment companies) information about customer transactions or personal information based on the existence of the entity's logo located on some banking products, such as credit cards.³³¹ Circular number (33703), however, was issued because SAMA has received many questions from the banks about what consumer

³²⁸ Banking Consumer Protection Principles SA §5/1 (2013)

³²⁹ Banking Consumer Protection Principles SA §5 (2013)

³³⁰ I tried to contact SAMA to obtain the unpublished administrative circulars, but the employee sent me what are already on SAMA's website.

³³¹ SAMA administrative circular #14547 on 2/22/2011 Available at <http://www.sama.gov.sa/ar-sa/Laws/BankingRules/IND-14547-1432H.pdf>.

information banks can freely disclose.³³² SAMA clarified that the previous circulars meant to protect any information that might directly or indirectly affect trust and bank secrecy, which may jeopardize the interests of Saudi Arabia, the bank, its customers, investors, or employees.³³³ On the same circular, SAMA instructed banks to task their respective legal departments with reviewing all requests related to the disclosure of customers' information before giving up the information.

Further, article 9 of BCPP, which is entitled "Data Protection and Confidentiality," holds the banks accountable for protecting and maintaining the confidentiality of consumer data even if the data is held by a third party.³³⁴ Banks have to provide a safe and confidential environment to ensure the privacy of consumer data.³³⁵ No further instructions have been given that describe the safe and confidential environment specifications. Additionally, banks shall not disclose consumers' personal information except when a relevant authority seeks the information or when the bank has written consent from the consumer.³³⁶ Lastly, banks shall ensure that only authorized employees are able to access and use consumers' personal information.³³⁷

As such, the Banking Consumer Protection Principles were created to protect customer privacy. The ambiguity of these principles and circulars, however, is reflected in the numerous questions banks have had regarding what constitutes information that may be disclosed.

³³² Administrative circular #33703 on 6/15/210, available at <http://www.sama.gov.sa/ar-sa/Laws/BankingRules/IND-33703-1431H.pdf>.

³³³ Administrative circular #33703 on 6/15/210, available at <http://www.sama.gov.sa/ar-sa/Laws/BankingRules/IND-33703-1431H.pdf>.

³³⁴ Banking Consumer Protection Principles SA §9/1 (2013). The Banking Consumer Protection Principles define a third party as "An authorized agent acting on behalf of the bank."

³³⁵ Banking Consumer Protection Principles SA §9/2& 9/4(2013)

³³⁶ Banking Consumer Protection Principles SA §9/3(2013)

³³⁷ Banking Consumer Protection Principles SA §9/5(2013)

Accordingly, SAMA has directed banks to consult with their legal departments to interpret the provisions of the Principles. In addition to the generality of the principles and the difficulty of interpreting them, many of the rules that are supposed to protect consumers' privacy are not published such that consumers can actually access them. Therefore, practically, SAMA is currently the only body that can oversee banks, interpret the principles, and issue penalties to those banking institutions that violate the principles.

➤ **The Law of Practicing Healthcare Professions and its Implementing Regulations**

Similar to the legal protection of individuals' privacy afforded via the BCPP, the Law of Practicing Healthcare Professions (LPHP) has established broad rules aimed at protecting individuals' health information. Article 21 of the law requires that a healthcare professional shall maintain the confidentiality of information obtained in the course of his or her practice and may not disclose it without written consent from the concerned party except if the disclosure was to report a case of death resulting from a criminal act, to prevent the commission of a crime, or to report epidemic diseases.³³⁸ Violators of the confidentiality requirements may be subject to a fine of not more than 20,000 SR (approximately \$5,333 USD) in addition to other disciplinary sanctions such as the revocation of a professional license. These penalties can be increased depending on the severity or frequency of the offense.³³⁹ Any lawsuit regarding the violation of privacy as it pertains to health information will be heard by a committee formed according to a decision made by the Minister of Health.³⁴⁰

Still, several details remain unclear regarding the collection, disclosure, and use of patient health information in Saudi Arabia. For example, the law does not specify how health

³³⁸ Law of Practicing Healthcare Professions SA §21 (2005).

³³⁹ Law of Practicing Healthcare Professions SA §30&31&32 (2005).

³⁴⁰ Law of Practicing Healthcare Professions SA §21 (2005).

information can be used, disclosed, and transferred. Thus, most hospitals and clinics, both public and private, tend to establish their own broad policies regarding patients' right to privacy.³⁴¹ King Faisal Specialist Hospital & Research Center (KFSH&RC), however, is an exceptional example of a hospital that has a written privacy policy with a high degree of clarity and detail.³⁴² The policy clarifies the conditions in which KFSH&RC may use and disclose a patient's health information, such as when treatment is necessary, when the patient is a part of medical research, or when there is a billing matter to address.³⁴³ In addition, KFSH&RC's privacy policy indicates patients' rights regarding their health information. These rights include the patient's right to address accounting matters; to amend, inspect, and obtain copies of records; to request restrictions; and to request confidential communications. The policy outlines the procedures for exercising each of these rights. Regardless of the relatively well-written policy, which is a rare example, KFSH&RC can make policy changes at any time, and the changes could apply to medical information that KFSH&RC already has about its patients.³⁴⁴ Ultimately, despite the importance and sensitivity of health information, the situation in Saudi Arabia remains ambiguous, as it is being addressed by broad rules and principles.

➤ **The Draft Law of E-Commerce (2014)**

Even though Saudi Arabia's e-commerce sector is growing rapidly and the government is pushing toward greater investment in the e-commerce market, there has been no comprehensive

³⁴¹ See Specialized Medical Center, Patient's Bill of Rights, https://www.smc.com.sa/main/index.php?option=com_content&view=article&id=72&Itemid=92&lang=en (last visited Nov. 10, 2018); Ministry of National Guard Health Affairs, Patient Rights, <http://ngha.med.sa/English/Patients/Pages/PatientsRights.aspx> (last visited Nov. 10, 2018).

³⁴² King Faisal Specialist Hospital & Research Center, Notice of Privacy Practices, <https://www.kfshrc.edu.sa/en/home/terms/noticeofprivacypractices> (last visited Nov. 10, 2018).

³⁴³ *Id.*

³⁴⁴ *Id.*

law established and implemented to govern e-commerce.³⁴⁵ The Ministry of Commerce and Investment drafted an e-commerce law in 2014, yet the law is still under revision. The law was last updated on July 3, 2018, when the Shura Council approved the draft.³⁴⁶ According to the ministry's spokesman Abdulrahman Alhusein, the proposed regulation will serve as a foundation upon which a trustworthy system supporting an online market can be built, as this will allow for regulation regarding online errors, online advertising, warranty guarantees, return policies, and the use of consumers' personal information.³⁴⁷ The drafted law is posted at the ministry's official website.³⁴⁸

The draft includes 27 articles. The second article explains the law's primary goals, which include enhancing the trust people place in the validity and integrity of e-commerce transactions; offering consumers protection against fraud, deception, and disinformation; and supporting and improving the e-commerce infrastructure in general. Protecting individuals' personal information was not directly mentioned as a primary goal. However, in article 15, the proposed law discusses some obligations regarding consumers' personal and banking information.

➤ **Article 15**

In this article, the law states, "A: no entity that obtains personal or banking data concerning a consumer may retain the data except for the period required by the nature of the

³⁴⁵ Generally see *Saudi Arabia's e-commerce market set to take-off*, OXFORD BUSINESS GROUP, at <https://oxfordbusinessgroup.com/analysis/expansion-horizon-favourable-forecast-kingdom%E2%80%99s-e-commerce-market> (last visited Nov. 13, 2018).

³⁴⁶ "Alshuraa" *Ywafq Ealaa Nizam Altijarat Al'iliktrunia [Shura Consul Approves E-commerce Law]*, ARGAM, Mar. 7, 2018, at <https://www.argaam.com/ar/article/articledetail/id/558128>.

³⁴⁷ Layan Damanhoury, *E-commerce law seen in Kingdom as online buying witnesses growth*, SAUDI GAZETTE, Aug. 2, 2017, available at <http://saudigazette.com.sa/article/514244/BUSINESS/E-commerce>.

³⁴⁸ MINISTRY OF COMMERCE AND INVESTMENT, E-COMMERCE LAW DRAFT, available at <https://mci.gov.sa/en/LawsRegulations/Projects/Pages/ProjectDetails.aspx?LawId=6bc74802-ba72-4fca-9253-a82500e26c79> (last visited Nov. 13, 2018).

transaction or may share the data with another entity, for or without payment, except if the entity is required or authorized by law or the entity has written permission from the consumer. B: The entity shall be responsible for any records that contain the customer's personal information or any records of the customer's e-communications, which are in its custody or under its control or with its agents or its employees, and shall take reasonable steps to ensure that the customer's personal information and related records are protected in a manner appropriate to its importance."³⁴⁹

The proposed law provides several legal protections with regard to consumers' data. First, entities are limited in terms of how long they may maintain consumers' personal and banking information; that is, they may not maintain it for a period longer than what the transaction actually requires unless the entities have obtained written permission from consumers. Second, the proposed law prohibits entities from sharing consumers' personal and banking information with other entities unless they have written permission from the consumer. Third, every entity that maintains a consumers' personal information is responsible for taking reasonable precautions, depending on the sensitivity of the data, to protect the personal information.

Although this article is considered a step forward in protecting people's private information, as it appears to do so in a number of ways, the language of the provision is a bit flawed, and this could be rectified by an executive regulation issued by the minister of commerce and investment.³⁵⁰ For instance, the law does not define "personal information." Defining personal information is critical if information is to be protected, and it could result in a conflict

³⁴⁹ Article 15 of E-commerce Law draft, SA (2014).

³⁵⁰ Article 27 states that the minister should issue executive regulations within 90 days after the law is enacted. Article 27 of E-commerce Law draft, SA (2014).

of interests is what constitutes personal information is left up to the entities' interpretations, which might vary.

Moreover, while the proposed law limits the period during which an entity may maintain or transfer consumers' personal information, it does not regulate the collection of personal information or the use of such information during the permitted period. As a result, companies might collect and use consumers' personal information beyond the intended purpose of the transaction without any legal ramifications. Additionally, the law holds entities responsible for protecting consumers' personal information, and it indicates that entities should put into place greater levels of protection when handling sensitive information. However, the law does not provide further explanation regarding the steps required to protect private information. The law also fails to state what precisely constitutes sensitive or important information. Furthermore, the proposed law indicates that the Ministry of Commerce and Investment is responsible for enforcing the law.³⁵¹ The ministry can issue a warning to the entity, and it can impose sanctions such as shutting down the website or issuing fines of up to one million Saudi Riyal, depending on the severity of the violation.³⁵²

Overall, the proposed law will offer individuals some protection regarding their private information by limiting the period during which entities are permitted to either retain consumers' personal data or transfer the information to third parties. However, not defining essential terms such as "personal information" will create ambiguity, which will in turn lead entities to come up with their own understandings. Executive regulation could serve to address this ambiguity and provide clarification.

³⁵¹ Article 20 of E-commerce Law draft, SA 2014

³⁵² Articles 22 & 23 of E-commerce Law draft, SA 2014

➤ **Civil Affairs Law (1986)**

With regard to information considered confidential or personal per Saudi laws, the Civil Affairs Law classifies some individuals' personal information as confidential and explains how the government shall handle such information. The Saudi Civil Affairs Law requires that every Saudi citizen at least 15 years of age must obtain an identification card.³⁵³ The law indicates the penalties associated with not obtaining an identification card.³⁵⁴ The law also requires every householder to obtain a "family book," which has information about all of his family members. The identification card contains the person's name, date of birth, a photograph, the individual's place of registration, and an ID number.³⁵⁵ Other detailed information, such as the individuals' parents' names, social status, level of education, and occupation, are stored at the Civil Affairs Offices and do not appear on the identification card or in the family book.³⁵⁶

The Civil Affairs Law considers individuals' civil records to be extremely confidential documents. Thus, according to article 11, the records shall not be, in any case, transferred from the Civil Affairs Offices. If a judicial authority issues a decision to review some of these records, a delegated judge or formal investigator must visit the place where the records are stored to review these records.³⁵⁷ The law places emphasis on protecting records in general by making access to the records difficult rather than by categorizing information in terms of confidentiality. As a result, many government agencies still disclose some information found in the civil records. For example, the execution courts³⁵⁸ announce some of their rulings by publishing them in local

³⁵³ Civil Affairs Law SA §67 (1986).

³⁵⁴ Civil Affairs Law SA §81 (1986).

³⁵⁵ Besides the information on the identification card, the family book contains the family members' names, date of birth, place of birth, and ID number.

³⁵⁶ Al-Qahtani, *supra* note 220 at 494.

³⁵⁷ Civil Affairs Law SA §11 (1986).

³⁵⁸ Courts competent in enforcing final judgments issued by other courts.

newspapers. The full name and ID number of the sentenced person are often posted in the announcement.³⁵⁹ Disclosing this type of information may pose a threat to the privacy of the citizen, yet there is no clear or precise legal provision that states that disclosing such information is an invasion of an individual's privacy.

❖ Conclusion

After examining most of the provisions of the Saudi laws that provide legal protection of individuals' information privacy, it is evident that Saudi legislators notably tend to use broad language when attempting to regulate matters related to information privacy. For example, the Anti-Cybercrime Law incriminates any "invasion of privacy through the misuse of a camera-equipped mobile phone and the like," and any "production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through an information network or computer" without explaining what constitutes an invasion of privacy. Further, the E-Transaction Law and its executive regulation provide some protection regarding electronic data in general without granting personal information extra legal protection. The Telecommunications Law and its executive regulation, however, might be the most sophisticated and detailed law aimed at protecting information privacy because it limits service providers' abilities to collect, disclose, and use consumers' information without their prior consent or legally grounded authority. Additionally, the Telecom Law gave the Communications and Information Technology Commission jurisdiction in cases that involve service providers violating customers' privacy.

Due to the number of loose legal provisions aimed at protecting individuals' privacy,

³⁵⁹ *Mahkamah Altanfidh Bialriyad Tamahal Saad Alhariri 5 'ayam [Court of Execution in Riyadh Gave Saad Hariri Five Days to Implement a Judicial Decision]*, JAZAN NEWS, DEC. 15, 2016, at <http://www.jazannews.org/news.php?action=show&id=45333>.

judges of the Sharia courts are left with considerable discretion in determining what constitutes violation of individuals' information privacy. The next chapter clarifies why the current level of protection of personal information in Saudi Arabia is insufficient and ineffective.

Chapter 3: Why is Saudi Arabia's current level of protection regarding individuals' private information deficient and thus ineffective?

❖ Introduction

The previous two chapters discussed the legal protections both Sharia law and Saudi legislation have afforded individuals with regard to information privacy. This chapter discusses why the current level of privacy provided to individuals regarding their personal information is lacking and thus why the protections provided via both Sharia principles and Saudi legislation are not sufficient enough to ensure the privacy of individuals' information in the digital age. More specifically, this chapter discusses the seven primary obstacles that affect the current level of protection provided to citizens. First, there is no comprehensive law in place that addresses the protection of individuals' personal data, and this has resulted in ambiguity as it applies to privacy and the law. Second, the Saudi courts' decisions regarding claims for compensation for moral damages have been inconsistent. Third, applying general Sharia principles to decisions regarding contemporary digital issues requires judges with specific qualifications, which are rare among judges in Saudi Arabia. Fourth, regardless of judges' qualifications, it is not an option to develop the information privacy system via the courts' decisions, as these decisions are not regularly published such that the public can access them, and the decision of one court is not binding in other courts. Fifth, the Saudi legal system does not recognize class action lawsuits. Sixth, Saudi citizens are not fully aware of their privacy rights. Finally, there is a scarcity of legal professionals specializing in privacy laws. The next chapter suggests solutions aimed at increasing citizens' information privacy protection in Saudi Arabia.

❖ **The primary obstacles affecting the insufficiency of the current level of information privacy protection in Saudi Arabia**

➤ **Obstacle 1: The absence of a comprehensive data protection law**

The previous chapter presented an overview of the legal protection of individuals' information privacy achieved via Saudi legislation. It showed that the legal protection is spread out over several legislative instruments. Although most of these laws do not address privacy as one of the main concerns of the law, they still provide some legal protection of individuals' information privacy. No comprehensive law focuses primarily on information privacy, however. Moreover, the language of most of the rules tends to be very broad whenever addressing information privacy concerns. The absence of laws concerned primarily with protecting information privacy and the broad and weak language used in current laws that address information privacy have resulted largely in a state of ambiguity as it relates to the current situation regarding protection of privacy.

In the absence of comprehensive and clear data protection laws, the Saudi courts are left with considerable discretion that enables them to address claims of privacy violation via general Sharia principles. This would not be an issue if the cases involved standard legal issues, such as divorce, physical violence, or sales, because the classical Islamic jurists discussed these matters in great details in their books. Thus, it would not be an issue for a judge to decide on one of these classic cases based on the principle of Sharia law. However, as noted in the second chapter, this is not so when matters of privacy are at the center of a case, especially if the issue at hand is related to the digital world. Sharia principles that apply to privacy matters tend to be general in nature; therefore, if a judge is to reach a conclusion based on these general principles, then the

judge must have obtained certain high qualifications (i.e., Mujtahid).³⁶⁰ In addition, since matters regarding information privacy are heard not only by General Sharia courts, some of the judges who are going to decide on privacy matters might not have sharia background at all.³⁶¹

Further, in the absence of comprehensive information privacy law, cases related to information privacy are spread out among several courts and committees such as General Sharia Courts; Criminal Courts; the Board of Grievances; the Banking and Financial Disputes and Violations Committee; and the Healthcare Professions Violations Committee.

For example, criminal courts are tasked with making decisions regarding compensation sought as a result of Anti-Cyber Crime Law violations. According to article 15 of The Anti-Cyber Crime Law, the public prosecution shall be responsible for the investigation and prosecution of the crimes stipulated in this law.³⁶² If an individual's private information is also violated according to the Anti-Cyber Crime Law, the harmed person may seek compensation by filing a claim with the public prosecutor during the criminal investigation.³⁶³ Additionally, the harmed person reserves the right to seek compensation before the criminal court even if the public prosecutor has rejected his or her request during the investigation.³⁶⁴

However, if an individual's information privacy is being compromised as a result of a

³⁶⁰ On the third obstacle, I will explain the required skills and whether the Saudi Judges are qualified to draw a conclusion based on the general Sharia principles or not.

³⁶¹ On the third obstacle, I will explain which courts might face the issue of having a judge with no Sharia background.

³⁶² The Anti-Cyber Crime Law, SA §15(2007).

³⁶³ Article 68 states, "Whoever suffers harm in consequence of a crime may file a claim in respect of his private right of action during the investigation of that action. The Investigator shall decide on the admissibility of such claim within three days from the date of filing. If the claim is rejected, an appeal may be lodged with the head of the relevant department within one week from the date of communication of the decision to the interested party. The decision issued by the head of the relevant department shall be final during the investigation stage." Law of Criminal Procedures, SA §68 (2013).

³⁶⁴ Article 148 states, "A person harmed by a crime and his heirs shall, at any time during the proceedings of the case in issue, be entitled to submit a request to the trial court regarding his private right of action regardless of the amount thereof, even though his action has been rejected during the investigation." Law of Criminal Procedures, SA §148 (2013).

violation of the Telecommunications Law or its Executive Regulation, the Communications and Information Technology Commission (CITC) has the authority to handle complaints between users and service providers and to decide whether the service provider violated the Telecommunications Law or its Executive Regulation. If the service provider has violated the law, the commission might issue a fine of up to 25 million Riyal.³⁶⁵ The commission's decisions are limited to fines and sanctions. The commission is not authorized to award compensation to the harmed person. Thus, the harmed person will need to file another complaint before the Sharia General Courts in order to seek compensation for his or her losses or damages.³⁶⁶ Lastly, the concerned party might appeal the commission's decision to the Board of Grievances (administrative courts).³⁶⁷

Furthermore, if a bank violates the Banking Control Law, Banking Consumer Protection Principles, or an agreement between an individual and the bank by unlawfully using a person's private information, the case shall be brought before Banking Disputes and Violations Committee (BDVC).³⁶⁸ Unlike the CITC, the BDVC has the authority to award compensation to the harmed party. Additionally, the concerned party might appeal the BDVC's decision to another committee called the Appeals Committee for Banking Disputes and Violations. The

³⁶⁵ The Executive Regulation for the Committee to Consider Violations of the Telecommunications Law, SA §9 (2002)

³⁶⁶ The Communications and Information Technology Commission is working to amend the Telecommunications Law to extend the commission jurisdiction to include the compensation cases beside the sanctions. See Modhi Almutairi, *Hyiat Alaitisalat" l "alaitisadia": Sharikat Jadidat Satadkhul Alsuwq Qaribaan Wataewidat Lilmutadaririn [Communications Authority" for the "Economic": a new company will enter the market soon .. and compensation for the affected]*, ALEQTISADYAH, Apr. 14, 2017, available at http://www.aleqt.com/2017/04/13/article_1169366.html.

³⁶⁷ Article 39 states, "The Commission's decisions can be appealed to the Minister. If the Minister upholds the Commission's decision, the concerned party has the right to appeal to the Grievance Dewan according to its Act." Telecommunications Law, SA §39 (2001).

³⁶⁸ According to Royal Decree (8/729) on 10/7/1407H and Royal Decree (37441) on 11/8/1433H, BDVC has jurisdiction over any case involves a bank.

decision of the appeals committee is a final decision.³⁶⁹

With regard to medical information held by healthcare professionals, the Law of Practicing Healthcare Professions (LPHP) has established rules aimed at protecting individuals' health information.³⁷⁰ If a healthcare professional violates these rules, a committee will be assigned by the Health Minister to decide any case based on the violation of the LPHP.³⁷¹ The Commission's decisions may include compensation for the harmed party and are subject to appeal before the Board of Grievances.³⁷²

Finally, the Board of Grievances is an administrative court that has jurisdiction over any case involving the government as a party,³⁷³ while the General Sharia Courts have jurisdiction to decide all cases unless law exempts that case.³⁷⁴ As a result, information privacy cases might go to one or more of six different courts in Saudi Arabia. Each one of these courts has established unique principles and rules, and the judges of these courts come from different backgrounds.³⁷⁵ The multiplicity of courts that are entitled to hear cases concerning the protection of individuals' personal data, as well as the judges' considerable discretion to deal with claims of privacy violations under the broad Sharia principles, underscore the ambiguous and inconsistent nature of the courts' decisions.

³⁶⁹ Royal Decree (8/729) on 10/7/1407H and Royal Decree (37441) on 11/8/1433H

³⁷⁰ Law of Practicing Healthcare Professions SA §21 (2005)

³⁷¹ Law of Practicing Healthcare Professions SA §38 (2005)

³⁷² Law of Practicing Healthcare Professions SA §38 (2005)

³⁷³ Law of the Board of Grievances, SA §11 (2007)

³⁷⁴ Article 25 states, "Without prejudice to the provisions of the Law of the Board of Grievances, the courts shall have jurisdiction to decide all cases in accordance with the rules governing the jurisdiction of courts set forth in the Law of Procedure before Sharia Courts and the Law of Criminal Procedure." Law of Judiciary SA §25 (2007).

³⁷⁵ For example, the members of the Banking Disputes and Violations Committee, Communications and Information Technology Commission, and the committee assigned by the Minister of Health to decide the violations of Law of Practicing Healthcare Professions do not require to have Sharia background. Whereas the judges in Board of Grievances courts, Criminal Courts, and General Sharia Courts are required to have at least a Bachelor degree in Sharia Law.

➤ **Obstacle 2: The Saudi courts' decisions on compensation for moral damages are inconsistent**

Compensation for moral damages is a cornerstone when it comes to information privacy. Most data protection violations result in moral damages, such as distress, rather than immediate material damages.³⁷⁶ Multiple courts have jurisdiction over the same issue when one is seeking compensation for moral damages. Thus, this dissertation chose to examine the inconsistent nature of compensation for moral damages in the Saudi courts so as to discuss how it suggests the lack of adequate information privacy protection in Saudi Arabia.

Any compensations granted by the Saudi courts must comply with Sharia principles, as stated on the Saudi Basic Law.³⁷⁷ Compensating moral damages remains controversial in Sharia. The second chapter of this dissertation indicates what Sharia's scholars have said about whether or not the morally harmed person is eligible for compensation. Most Sharia scholars believe that the morally damaged person should not be awarded compensation because it is difficult to estimate the magnitude of moral harm, and it is therefore difficult to determine what serves as a fair compensation. As a result, Saudi courts have rarely awarded compensation for moral damages.³⁷⁸

Still, the Saudi courts do not always refuse to compensate individuals for moral damages. Recently, some courts began awarding moral damages in some cases. Ten years ago, the administrative courts at the Board of Grievances began recognizing moral harm when it is combined with material damages.

³⁷⁶ Damian Clifford & Yung Shin Van Der Sype, *Online dispute resolution: Settling data protection disputes in a digital world of customers*, 32.2 Computer Law & Security Review 272, 274-275 (2016).

³⁷⁷ *KSA Courts Open the Door to Moral Damages*, CLYDE & CO, Dec. 21, 2015, available at <https://www.clydeco.com/insight/article/ksa-courts-open-the-door-to-moral-damages>.

³⁷⁸ *Id.*

- 1- The administrative court at the Board of Grievances decided that the claimant is entitled to compensation because he was illegally arrested for 239 days. The court in its reasoning described the material and the moral damages caused by the unlawful arrest. The material damage is the loss of money due to the absence of work during the arrest. The court also mentioned psychological pain, which is the distortion of reputation and the sense of humiliation because of the illegal detention. However, the court estimated the compensation based on the prisoner's financial condition before being he was imprisoned as well as while he was imprisoned. Thus, if before the arrest, the prisoner had a monthly salary of 10850 Riyals, which was earned for work completed seven hours per day, the court determined the arrested wage per hour and added 17 hours (to account for the rest of the day) at the same rate to come up with the total compensation.³⁷⁹
- 2- The administrative court at the Board of Grievances awarded an individual with 2000 Riyal because the General Directorate of Passports detained him for 24 hours without a legitimate reason. The reasoning explained that the compensation was to compensate the individual for moral and the material damages.³⁸⁰

Notably, the court-awarded compensation in both of these examples served to compensate for both material and moral damages. For the cases that involve only moral damages without any material damages, the courts have been reluctant to compensate individuals. In 2008, the appeals court at the Board of Grievances refused to compensate a morally harmed person, reasoning that the moral harm alone could not be logically

³⁷⁹ Case: 747/1 On 1427H

³⁸⁰ Al-Qahtani, *Supra* note 7 at 131.

estimated.³⁸¹

However, in 2015, the administrative court at the Board of Grievances issued a final decision against an airline responsible for causing a family moral damages.³⁸² The harm occurred during a domestic flight when one of the daughters within the family was seated on a dirty seat. The daughter's clothes and body remained unclean during the flight, and the flight attendant had to change the daughter's seat. The court decided that the family was entitled to compensation because the dirty seat caused the family to experience psychological pain, including the stress the parents experienced after their daughter's seat was changed, as this made the act of supervising the daughter more difficult. The court based its decision on Sharia principle and concluded that the airline was responsible for compensating each member of the family with 4000 Saudi Riyal even though the price of the flight ticket was only between 575 to 635 Saudi Riyal, as stated on the judgment the appeals court upheld the decision.³⁸³

In the same year, the Board of Grievances conducted a workshop for the judges, titled "Compensating Moral Damages in Saudi Arabia." The workshop concluded that compensating moral damages is permissible in accordance with Sharia principles. The airline's case and the workshop's recommendations suggest that Saudi administrative courts might begin recognizing moral damages as a reason for compensation.

Nevertheless, it is important to mention that the workshop recommendations are merely directive and the appeals court decisions are not binding to the lower courts.³⁸⁴ Thus,

³⁸¹ Case: 1/815 On 1428H

³⁸² Case: 4/519 On 1435H

³⁸³ Case: 4/519 On 1435H

³⁸⁴ *Alqada' Al'iidariu Yastaqbil Daeawaa Aldarar Almaenawii [Administrative Courts Receive Cases of Moral Damage]*, MAKKAH NEWSPAPER, Oct. 10, 2015, at <https://makkahnewspaper.com>.

a judge can still reject moral damages compensation based on Sharia law, which still views compensation for moral damage as a controversial issue.

All of the progress the courts have achieved regarding compensation for moral harm has occurred within the Board of Grievances, which has jurisdiction exclusively over all disputes to which the government is a party. The General Sharia Courts and other committees still have not published any cases whereby the court awarded compensation for moral damages.

Thus, because information privacy violations often lead to moral damage rather than material damage, it might be difficult for the harmed party in Saudi Arabia to seek and achieve compensation for information privacy violations. If someone's personal information has been compromised, and he or she has proven that harm has occurred after a violation of one of the Saudi regulations or Sharia law, the harmed person will most likely not receive any compensation. The court will probably decide only to punish the violator with sanctions or other means of punishment. This might be one of the primary reasons behind the scarcity of causes related to information privacy in Saudi courts.

The absence of a law that compels judges in Saudi Arabia to consider compensating individuals for moral harm will serve to perpetuate the issue. The judges in both General Sharia Courts and the Board of Grievances are not presently required to consider any case involving moral damages, and the judges can back their opinions with rational Sharia principles. The judges might not see the big picture or the necessity of considering moral harm as it relates to information privacy violations, and they are not obligated to do so. Due to the continued lack of consistency regarding the compensation for moral harm suffered in Saudi Arabia, the option to file a complaint before the Saudi courts regarding an information

privacy violation will remain fraught with many problems and risks, including the broad language of the laws that protect information privacy and the low probability of that the individual will receive compensation even after he or she proves that a violation occurred.

➤ **Obstacle 3: Sharia Principles are too broad to address privacy concerns in the digital world, and most of the Saudi judges are not qualified as a mujtahid**

The second chapter “Privacy in Islam” introduced the main principles meant to protect individuals’ privacy. The principles include: 1) prohibiting any intrusion, regardless of how the information is obtained, to individuals’ homes, papers, or confidential conversations; 2) establishing a new set of rules that regulate how to seek permission before entering someone’s house or coming between two people who appear to be having a confidential conversation in a public place; 3) maintaining the confidentiality of the individual's private information by incriminating any disclosure of any information that may lead to harm of another person, and the order to conceal others’ private information, especially confidential information that appears through a certain necessity such as a physician-patient relationship or a husband-wife relationship. These principles were able to deliver a high level of protection of individuals’ privacy when Islam was newly emerged. Using broad language and relying on the general custom made it possible for these old principles to be readily applied in innumerable contexts.

Today, however, thanks to the technological revolution, the amount of personal information available has increased considerably. Further, it has become much easier to access individuals’ personal information, which poses an unprecedented risk to individual privacy. The Sharia principles and rules that protect information privacy need to be further developed so that they can provide individuals in a post-digital era with the same level of privacy protection they provided during the pre-digital era. The Sharia principles could be employed as a means of

addressing contemporary privacy issues in two ways: 1) written laws could be drawn from these principles, and 2) judges could directly apply these principles to make decisions regarding new issue via *Ijtihad*.³⁸⁵

The third chapter of this dissertation discussed the lack of written laws aimed at protecting information privacy in Saudi Arabia and how the extant rules tend to use broad language rather than detailed provisions. As such, the first potential means of employing the Sharia principals is not exercised in Saudi Arabia at present.

This section examines the possibility of protecting individuals' information privacy in Saudi Arabia via judges who can apply the Sharia principles in order to make decisions regarding non-regulated issues. The majority of three Islamic schools (i.e., Maliki, Shafi'i, Hanbali) require that a judge must be recognized as mujtahid in order to be assigned as a judge.³⁸⁶ A mujtahid is "one who exercises independent reasoning (ijtihad) in the interpretation of Islamic law. Qualifications include training in recognized schools of Islamic law and extensive knowledge of the *Quran* and hadith."³⁸⁷ According to Wael Hallaq, ijtihad is the highest effort put forth by Sharia scholars to master and apply the principles and rules of legal theory for the purpose of discovering God's law.³⁸⁸ An essential characteristic of the mujtahid is that the mujtahid has to be able to recognize the most valid opinion from among the different Islamic schools.³⁸⁹ Thus, the mujtahid is supposed to have a background linked to multiple

³⁸⁵ This term will be explained later in this section.

³⁸⁶ NASSER ALMIMAN, ALNWAZIL ALTASHRIYAH 51(1999).

³⁸⁷ See Intisar A. Rabb, *Ijtihad*, OXFORD ISLAMIC STUDIES ONLINE, available at <http://www.oxfordislamicstudies.com/article/opr/t125/e1596> (last visited Nov. 13, 2018).

³⁸⁸ Wael B. Hallaq, *Was the Gate of Ijtihad Closed?*, 16 International Journal of Middle East Studies 3–41 (1984).

³⁸⁹ RESEARCHES OF THE SENIOR SCHOLARS, V.3 at 180 (2001), available at <http://www.alifta.net/Fatawa/fatawaChapters.aspx?languagename=ar&View=Page&PageID=287&PageNo=1&BookID=1>.

Islamic schools. Further, it may be worth noting here that there is no place for *ijtihad* when there is a clear text from the Quran or Sunnah because the law is definite in these instances, and *ijtihad* is reserved for instances of ambiguity.³⁹⁰ Thus, *ijtihad* becomes more important when the legal texts are not explicit and when the principles are broad and can be interpreted in different ways, such as is the case regarding new information privacy issues.

On the other hand, the majority at Hanafi School and a minority at Maliki School believe that a judge can be *Muqallid* even when the judge is not qualified to practice *ijtihad* but can decide the case based on following mujtahids.³⁹¹ *Taqlid* follows a mujtahid's opinion regarding an issue because of the inability to practice *ijtihad*.³⁹² Most modern jurists from all of the four schools believe that it is permissible to appoint a judge who is classified as *muqallid* if there is no mujtahid.³⁹³

This brings us back to the central question, however, regarding whether Saudi judges are able to protect individuals' privacy by applying the Sharia principles in order to address non-regulated information privacy matters. The answer to this question depends on whether the Saudi judges are classified as mujtahid or *muqallid*. There is no specific study or standardized test that determines precisely whether a judge is a mujtahid or *muqallid*. Therefore, to answer this question, one may have to look at two factors: 1) the judge's educational background, and 2) the evaluation of the Council of Senior Scholars, the highest religious institution in Saudi Arabia, regarding the levels of current judges.³⁹⁴

³⁹⁰ John L. Esposito, *Ijtihad*, THE OXFORD DICTIONARY OF ISLAM, available at <http://www.oxfordislamicstudies.com/article/opr/t125/e990> (last visited Nov. 13, 2018).

³⁹¹ Almiman, *supra* note 386 at 51.

³⁹² Bernard G. Weiss, *Taqlid*, OXFORD ISLAMIC STUDIES ONLINE, available at <http://www.oxfordislamicstudies.com/article/opr/t236/e0785> (last visited Nov. 13, 2018).

³⁹³ Almiman, *supra* note 386 at 59.

³⁹⁴ Council of Senior Scholars was founded in 1971. The king selects the members of the council. The council's primary purpose is to advise the king on Sharia matters.

According to The Law of the Judiciary, each judicial candidate is required to hold a degree from one of the Sharia Schools in Saudi Arabia.³⁹⁵ A judge must also be at least 22 years of age in order to be appointed to first-degree courts and at least 40 years of age to serve as an appellate judge.³⁹⁶ To help the judges to reach a higher level of education, Saudi Arabia has established a Judicial Academy and an Institute of Public Administration to prepare judges, expand their knowledge, enhance their skills, and provide them with the information that they need to work effectively.³⁹⁷ Attending the academy or the institution, however, is optional for the judges. Additionally, there is no test that must be taken to determine who is selected; selection is based solely on personal interviews.³⁹⁸

What follows is an example of the academic plan of the Sharia School at Imam Muhammad ibn Saud Islamic University, one of the world's most elite Sharia schools and a school from which a considerable number of judges in Saudi Arabia have graduated. Presentation of this academic plan allows for a closer look at the judges' educational background. The example will show:

- 1- The courses
- 2- Whether the course is directly related to judicial work or not based on the course description
- 3- Number of hours per course

³⁹⁵ The Law of the Judiciary, SA §31. (2007).

³⁹⁶ The Law of the Judiciary, SA §31. (2007).

³⁹⁷ See Abdullah ALAnsary, *Judges' Qualifications, Job Performance and Training*, GLOBAL LAW AND JUSTICE, at http://www.nyulawglobal.org/globalex/Saudi_Arabia1.html#_Toc424144441 (last visited Nov. 13, 2018).

³⁹⁸ According to article 31 of The Law of the Judiciary, "(d) He shall hold the degree of one of the Sharia colleges in the Kingdom or any equivalent degree, provided that, in the latter case, he shall pass a special examination to be prepared by the Supreme Judicial Council." The Law of the Judiciary, SA §31. (2007)

4- School of jurisprudence, the courses of which were chosen³⁹⁹

Not Directly related to the judiciary		Directly related to judiciary or not		
The course	hours	The course	hours	Curriculum & School
The Noble Quran	8	History of Jurisprudence	2	<i>almdkhl llykh alislami tarikh alfkh alislami almlkiah wnthriah ala'kd</i> (Introduction to Islamic Jurisprudence) , Hussein Ahmed,
Exegesis of the verses of Judgment	13	Legal Judgment	3	<i>Rawdah Alnazer wa Janah Al-Mnazer</i> , Ibn Qudamah (died: 1223) (School: Hanbali)
Prophetic Traditions of Worships	6	Evidence of Judgment	13	<i>Rawdah Alnazer wa Janah Al-Mnazer</i> , Ibn Qudamah (died: 1223) (School: Hanbali)
Monotheism	11	Prophetic Traditions of Treatment	2	<i>Subil alsalam fi sharh bloq almaram</i> , Alsanani (died: 1768) (School: Shafi'i)
Jurisprudence of Worships	15	Jurisprudence of Treatment	9	<i>Alrawd AlMurbe fi Sharh Zad Al-Mustaqni</i> , al-Bahūtī (died:1641) (School: Hanbali)
Hadith Terminology	2	Higher Objectives of Sharia	2	<i>Almuwafqat</i> , Alshatbi (died:1641) (School: Malki)
Grammar	18	Introduction to laws	2	Introduction to Saudi Laws, Alrhahlh (2013)
The sciences of Qur'an	2	Islamic Sharia Politics	2	Introduction to Sharia Politics, Atwah (1993)
Values of Islam and its characteristics	2	Law of inheritance	7	<i>Altaḥqiqah almurdyah fi almabahith alfaradyah</i> , Alfwzan (1986) (School: Hanbali)
Computer sciences in Islamic Legal Studies	2	Islamic Jurisprudential Maxims	4	<i>Alashpah wa alnadaer</i> , Alsuyuti (died: 1505) (school: Shafi'i)
Hadith Ascription	1	Jurisprudence of Perpetration of Crime	2	<i>Alrawd AlMurbe fi Sharh Zad Al-Mustaqni</i> , al-Bahūtī (died:1641) (School: Hanbali)
Disagreement and Debate	2	Jurisprudence of Legal Punishments and Castigation	2	<i>Alrawd AlMurbe fi Sharh Zad Al-Mustaqni</i> , al-Bahūtī (died:1641) (School: Hanbli)
Arabic Composition	2	(Referring branches to	2	<i>Alqwaed wa alfawaed alosolyah</i> , Ibn Al-Lahim(died:1398)

³⁹⁹ Mohammad Bin Saud University, The Academic Plan for Sharia School, available at <https://units.imamu.edu.sa/colleges/sharia/Pages/tosifatnew.aspx> (last visited Nov. 13, 2018).

		Assets (Alusul		(School: Hanbli)
The Biography of the Prophet Muhammad	2	Hadiths of Legal Punishment and Judicial	2	<i>Subil alsalam fi sharh bloq almaram</i> , Alsanani (died: 1768) (School: Shafi'i)
Introduction to the Economy Science	2	Jurisprudence of Judiciary	3	<i>Alrawd AlMurbe fi Sharh Zad Al-Mustaqni</i> , al-Bahūtī (died:1641) (School: Hanbli)
Thinking skills OR Islamic Systems	2	Diligence (Independent Judgment)	3	<i>Rawdah Alnazer wa Janah Al-Mnazer</i> , Ibn Qudamah (died: 1223) (School: Hanbali)
History of The Kingdom	2	Judiciary Systems	2	Legislative power in Saudi Arabia, Almarsoqi, (2004)
		Jurisprudence of Contemporary Issues	2	<i>Fiqh alnawazil</i> , Almshiqh (2010)
Research Methods	2			
Hadiths of Family	2			
Semantic Indication	8			
Fundamentals of Islamic Education	2			
Practical Research Jurisprudence	1			
Professional Ethics	2			
Educational Psychology	2			
Curriculum and Teaching Methods	1			
Jurisprudence of Food and Oaths	2			
Religion and Sects	2			
Intellectual Contemporary Issues	2			
Administration and Policy of Education and Practicum	2			
Special Teaching Methods and Practicum	2			
Practical Research Islamic Culture	1			
Total	132 h		64 h	

The undergrad students of Sharia School have to study 82 courses, which total about 197 hours.⁴⁰⁰ More than 65 percent of the courses (132 hours of the 197) are not directly related to judiciary work. As such, the academic plan of the Sharia School at Umm Al-Qura University focuses on Sharia in general rather than on what the judges need to work effectively.⁴⁰¹ Moreover, most of the Sharia School curricula are chosen from old Hanbali School books.⁴⁰² Focusing on one school might be reasonable since judges in Saudi Arabia tend to apply Hanbali School in most of their judicial decision. However, as previously explained, the mujtahid is required to implement the most accurate opinion regardless of which school presented this opinion. Thus, Sharia schools in Saudi Arabia do not prepare a mujtahid judge who has the capacity to apply general Sharia principles when deciding novel issues.

The second factor that might determine the ability of Saudi judges to apply the Sharia principles in order to solve new information privacy disputes is the opinion of the Council of Senior Scholars with regard to the judges' current levels of education. In 2001, the King requested that the Council of Senior Scholars study the idea of codifying Islamic jurisprudence to reduce judges' discretionary powers that allow them to choose from among former jurists' opinions. Because there have been numerous different judgment outcomes regarding the same matter, the Saudi courts' decisions are unpredictable. The Council of Senior Scholars published their opinions in 2001. The scholars did not agree that Islamic jurisprudence should be codified. However, they agreed that most of the judges could not be classified as a mujtahid; they stated, "The level of education of most of the judges is weak, and they cannot practice ijthad by

⁴⁰⁰ *Id.*

⁴⁰¹ Umm Al-Qura University, The Academic Plan for Sharia School, *available at* <https://uqu.edu.sa/en/shreeahm/App/Plans> (last visited Nov. 13, 2018).

⁴⁰² The Sharia School at Imam Muhammad ibn Saud Islamic University teaches the Islamic jurisprudence through *Rawdah Alnazer wa Janah Al-Mnazer* and *Alrawd AlMurbe fi Sharh Zad Al-Mustaqni*. Both of these books are based on Hanbali School.

themselves and cannot consistently recognize the most accurate opinion from among the previous jurists' opinions."⁴⁰³ The council also believed that the disparity in judicial rulings resulted in the establishment of the different specialized committees, which took some of the Sharia courts' juridical authority away, making it increasingly difficult for the parties of a dispute to identify the court which has the qualitative jurisdiction.⁴⁰⁴ Finally, the scholars who disagreed with the idea of codifying Islamic jurisprudence emphasized that judges should receive better education and training, and the process of selecting the judges should be improved.⁴⁰⁵

However, members of the committees that have jurisdiction over some information privacy issues, such as the Banking Disputes and Violations Committee and the Communications and Information Technology Commission, might not have degrees in Sharia at all. For example, the committee tasked with decisions regarding violations of the Telecommunications Law or its Executive Regulation shall be formed by a decision of the Board of Directors of the Communications and Information Technology Commission and shall have at least one person who holds a degree in law.⁴⁰⁶ The law does not specify which degree a committee member shall hold, whether a degree in Sharia law or a law degree in general. Similarly, the committee tasked with decisions regarding violations of the Law of Practicing Healthcare Professions is required to have at least one member who has a law degree.⁴⁰⁷ Thus, some of information privacy cases will be considered via a committee whose members do not have backgrounds in Sharia. If graduates of Sharia schools are unable to practice *ijtihad*, graduates of law schools, which focus on

⁴⁰³ RESEARCHES OF THE SENIOR SCHOLARS, V.3 at 231(2001), *available at* <http://www.alifta.net/Fatawa/fatawaChapters.aspx?language=ar&View=Page&PageID=287&PageNo=1&BookID=1>.

⁴⁰⁴ *Id.*

⁴⁰⁵ *Id.*

⁴⁰⁶ The Executive Regulation of the committee that considers the violations of the telecommunications law and its procedures, SA §2 (2001).

⁴⁰⁷ Law of Practicing Healthcare Professions SA §38 (2005)

teaching the modern legal system rather than Sharia law, are also likely unable to exercise ijtehad.

What makes the situation more complicated is the scarcity of books and studies that discuss the new information privacy issues in accordance with Sharia principles. This increases the likelihood that a judge will look to the old Sharia books and try to use qiyas (an analogy) to come up with answers. Further, many of today's privacy issues are directly related to technology, and since no specific committee has jurisdiction over all of the data protection cases, all of the judges in the different courts and committees need to be properly trained to address modern digital privacy issues. However, this is not what is happening in Saudi Arabia, as indicated by the Sharia school academic plans. In addition, the law schools in Saudi Arabia do not offer any courses related to legal issues related to technology.⁴⁰⁸

Ultimately, applying broad Sharia principles to address data protection issues in the digital age will require a judge who is able to practice ijtehad. Neither students who graduated from Sharia schools nor those who graduated from law schools in Saudi Arabia are qualified to exercise ijtehad. Therefore, any new issues associated with technology that the Islamic jurists have not discussed in their book will be difficult for Saudi judges to consider or to decide on based on Sharia principles. Having Sharia principles that offer protection to individuals' information privacy is not enough if the judges are incapable of applying these principles to the issues.

⁴⁰⁸ King Saud University, The Academic Plan of Law School, *available at* <https://clps.ksu.edu.sa/ar/node/298> (last visited Nov. 13, 2018); King Abdulaziz University, The Academic Plan of Law School, *available at* <https://law.kau.edu.sa/Pages-%D8%A7%D9%84%D8%AE%D8%B7%D8%A9.aspx> (last visited Nov. 13, 2018).

➤ **Obstacle 4: The judiciary system in Saudi Arabia does not recognize class action lawsuits**

A class action is a claim filed by one or more on behalf of a group of people who suffered similar harm from the same action.⁴⁰⁹ Class action lawsuit is a very helpful tool if the individuals' damages are relatively minor and each one of the harmed group is unable to afford to carry the lawsuit alone. Data breach is a perfect example of an issue where the class action lawsuit might serve as a very useful means of allowing individuals to seek compensation for damages because data breaches usually result in very low damages and the harmed party is a large group.⁴¹⁰ For example, according to the Ponemon Institute's 2014 study on data breach in the U.S., 43% of companies said that they had experienced data breaches involving the loss or theft of more than 1,000 records.⁴¹¹ In Saudi Arabia, the number of data breaches that have occurred is unknown because the companies are not obligated per Saudi law to notify their customers of a data breach.

The Civil Procedures Law in Saudi Arabia does not mention anything about class action lawsuits. Thus, if a lawyer wants to initiate a lawsuit for different people with similar damages from the same cause, the lawyer will have to file each lawsuit separately. Recently, the Saudi Capital Market Authority (CMA) issued a regulation that approves class action lawsuits. The law is special, however, and meant to apply to cases that fall within the Capital Market Authority

⁴⁰⁹ LAW.COM, CLASS ACTION, available at <https://thelawdictionary.org/legal-action/>.

⁴¹⁰ J. Thomas Richie, *Data Breach Class Actions*, 32 GPSolo 66, 12-13 (2015)

⁴¹¹ PONEMON INST, IS YOUR COMPANY READY FOR A BIG DATA BREACH? TAKEAWAYS FROM THE FIFTH ANNUAL STUDY ON DATA BREACH PREPAREDNESS 18 (2014), available at <https://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf>.

jurisdiction.⁴¹² Still, this could be seen as an encouraging step that may prompt other juridical entities to approve class action lawsuits as well.

Currently, in Saudi Arabia, even if an individual is aware that a company has had a data breach and therefore his or her personal information has been stolen by a third-party, the individual is not likely to assume the risks associated with suing the company and bearing the cost of the lawsuit alone, which might be more than what the individual would receive. This is especially true if compensation sought were related to only slight damages or non-material damages. The Saudi courts, as explained previously, do not usually recognize moral harm as a reason for compensation.

In short, a class action lawsuit is a useful tool to protect individuals' interests if their personal information has been compromised as a result of another party's negligence, etc. Additionally, the companies will likely take the act of protecting people's private information more seriously since a person would be able to initiate a massive lawsuit against the company.⁴¹³ Lastly, a sign of the importance of the class action lawsuit as a means of protecting individuals' privacy is that the recently adopted General Data Protection Regulation (GDPR) permits the class action suit for privacy violations.⁴¹⁴

⁴¹² *CMA approves Class Action Suit Regulations in securities disputes*, SAUDI GAZETTE, Nov. 22, 2017, available at <http://saudigazette.com.sa/article/522509/BUSINESS/CMA-approves-Class-Action-Suit-Regulations-in-securities-disputes>.

⁴¹³ Bryan Betts, *GDPR's latest gift? Class action privacy cases*, COMPUTER WEEKLY, Jan. 29, 2018, at <https://www.computerweekly.com/blog/Write-side-up-by-Freeform-Dynamics/GDPRs-latest-gift-Class-action-privacy-cases>.

⁴¹⁴ Joseph Srouji & Margaux Dolhem, *Class action and data privacy in the USA and Europe: Effective deterrent or ill-founded approach to compliance?*, 1.3 Journal of Data Protection & Privacy 294-305 (2017).

- **Obstacle 5: The courts' decisions are not regularly published such that the public can access them, and the decision of one court is not usually binding in other courts**

Another obstacle that has resulted in an inadequate level of information privacy protection in Saudi Arabia comes is also rooted in the nature of the Saudi legal system. Usually, when a country relies on board principles and rules, the court plays a critical role in shaping these rules and principles over the time. These common law system countries publish the cases and make the precedents binding in other courts. Thus, the next judges to hear cases with precedent will consider previous decisions as they come up with conclusions that will harmonize with the earlier judges' decisions. Generally, a judge will only contradict previous cases if there is a legitimate reason to do so.

In Saudi Arabia, before 2007, most of the juridical judgments that were available to the public were published unofficially by the parties' lawyers. Neither the Sharia court nor the administrative courts were making their decisions available to the public. This was a result of the prevailing opinion among the Sharia scholars, who did not give the precedent weight. According to the majority of jurists in the Islamic jurisprudence, the rule is that "the qadi (judge) must strive for the divine truth for each case that confronts him, without being bound by past opinions, even his own. Truth is the ultimate precedent to which one must return once it is revealed."⁴¹⁵ This encouraged a discrepancy in the judges' judgments, as the minister of justice has noted.⁴¹⁶ In 2002, the Council of Minister's decision number (162) came out stating that both the Ministry of Justice and the Board of Grievances have to select final decisions, review the decisions, and while protecting the privacy of the parties, they must publish these decisions so that they are

⁴¹⁵ FRANK VOGEL, ISLAMIC LAW AND LEGAL SYSTEM: STUDIES OF SAUDI ARABIA 15-16 (2000).

⁴¹⁶ *An Interview with The Minister of Justice*, ALSHARQ ALAWSAD, May. 2, 2009, available at <http://archive.aawsat.com/details.asp?section=43&issueno=11113&article=517451#.W-pxtBNKiRu>

available to the public.⁴¹⁷ Similarly, five years later, the King issued a Royal Decree requiring the Ministry of Justice and the Board of Grievances to select and publish some final judgments so that the public could access them. In 2007, both the Ministry of Justice and the Board of Grievances began releasing some of the courts' final decisions.⁴¹⁸ Since then, selective final judgments have been published. According to the introduction of a set of 1,200 judicial judgments published by the Ministry of Justice, the main reason behind the publication is to reduce the possibility that a discrepancy will exist with regard to judges' decisions.⁴¹⁹ Yet, no legal provisions bind the judges in Saudi Arabia to follow the rules of any other judges. The published decisions might be considered persuasive precedents.

The published cases were categorized by the subjects. For example, precedents released by the Ministry of Justice involved real estate, family law, contracts, and criminal cases. Cases published by the Board of Grievances were divided into administrative, criminal, and commercial matters. Among the officially published cases, however, only a few discuss privacy rights, and those that do were all criminal cases that had to do with violating the sanctity of someone's home or cybercrimes.⁴²⁰ None of the privacy cases had to do with data breach or inappropriately or illegally disclosing personal information.

Finally, as seen in the third chapter, with the absence of a specific law aimed at protecting people's information privacy, the judge will have to rely on the broad and general principles of Sharia law in order to decide a case. In addition to the inability of most judges to practice *ijtihad*,

⁴¹⁷ The Council of Minister's decision number (162) on 17/6/1423H.

⁴¹⁸ See THE SHARIA COURTS' PUBLISHED DECISIONS, MINISTRY ON JUSTICE, available at <https://www.moj.gov.sa/ar/SystemsAndRegulations/Pages/System1434.aspx>. See also THE BOARD OF GRIEVANCES COURTS' PUBLISHED DECISIONS, THE BOARD OF GRIEVANCES, available at <https://www.bog.gov.sa/ScientificContent/JudicialBlogs/Pages/default.aspx>.

⁴¹⁹ *Id.*

⁴²⁰ Some of these cases are about the intrusion of a house and the other fall under the Anti-Cybercrime Law.

their decisions are not binding to other courts. In another words, each judge faces a contemporary issue that does not fall under any of the Saudi laws, and the Sharia scholars have not discussed this issue. This means that the judge would have to decide the case via ijihad. If the same question were presented before another court later, the judge would probably have to search again and determine the dispute by exercising ijihad, as the judge would not know about the previous decisions or have access to a different opinion regarding the same issue. In short, it is true that case law plays a decisive role in filling the legislative vacuum in common law countries. However, in Saudi Arabia, although there is a legislative vacuum regarding the protection of individuals' information privacy, the role of the precedents remains marginal due to the low number of published cases and the absence of a legal provision that binds judges to consider these precedents.

➤ **Obstacle 6: Saudi citizens are not fully aware of their privacy rights**

Knowing how much members of Saudi society care about their privacy would likely be apparent via a tour of public places in Saudi Arabia. For instance, the partitions in the restaurants, the tall walls surrounding each home, and the many women who cover their faces for religious purposes are indicative of the society's concern for privacy. However, it is worth considering whether the society's concern about its right to privacy is reflected in the legal field. In another words, do people in Saudi Arabia know that their privacy is a guaranteed right protected by both Saudi laws and general principles of Sharia? Further, do members of the society know that they can seek to preserve their rights via the courts anytime they feel their right to privacy is being violated? This dissertation demonstrates that while Saudi society cares about its privacy, people in Saudi Arabia are not fully aware of their right to privacy.

- **Previous researches have attempted to measure the level of awareness**

In 2014, Alsulaiman and Alrodhan conducted a study to assess information privacy policies and practices in the public, health, banking, and private sectors.⁴²¹ As a part of the study, a survey was conducted to measure “awareness and perception of privacy issues related to clients, employees, and citizens,” as this was one of the primary purposes of the study.⁴²² The feedback revealed remarkable outcomes with respect to the level of awareness among individuals in Saudi Arabia regarding the privacy of their information. This dissertation sheds light on the most critical findings of the survey that may help to measure the level of people's awareness regarding the importance of information privacy.

- 1- Thirty-nine percent of the participants had never been asked to follow specific ‘privacy-protection’ procedures (and/or regulations) aimed at protecting the privacy of their organization’s clients/customers/users.
- 2- Only 38% of participants believed that private information that belonged to their organization's clients/customers/users was adequately protected. In the financial/banking sector, only 25% of participants believed that their organizations properly protected customers' private information.
- 3- Thirty-three percent said that they had come across a privacy-violation incident within their workplace. The percentage (41%) was higher in the financial/banking sector.
- 4- Regarding unauthorized access to customers’ private information by someone inside the organization, 34% of the sample had knowledge of such unauthorized access to private information that belonged to the organization’s clients/customers/users and/or personnel

⁴²¹ Laith Alsulaiman & Waleed Alrodhan, *Information Privacy Status in Saudi Arabia*, 7.3 Canadian Center of Science and Education (2014)

⁴²² *Id.* at 105.

without operational or justifiable reasons; only 25% reported the incident. surprisingly, none of the participants from the financial sector reported such incidents.

- 5- Of the participants, 84.16% considered themselves aware of the importance of privacy protection; however, only 50% were aware of IT Criminal laws in Saudi Arabia.
- 6- Eighty-four percent of participants believed that privacy protection is important.
- 7- Interestingly, 85% of the sample were not satisfied with the current level of privacy protection in Saudi Arabia; this was especially true among those who work in the financial sector.

Lastly, the paper emphasized the importance of raising the level of awareness regarding information privacy and concluded, “Country-level awareness initiatives are also needed to create the appropriate perceptions of information privacy and its importance from human rights and consumer standpoints.”⁴²³

Accenture published another paper that focused on information privacy in the healthcare sectors. It was noted that a significant majority of the consumers in Saudi Arabia trusted their healthcare providers to safeguard their personal information.⁴²⁴ The highest percentage of trust (79%) was for the government and hospitals, and the least trust (52%) was for non-medical staff at physicians’ or healthcare providers’ offices. Despite this high percentage of trust, the rate of consumers who have personally experienced a breach regarding their healthcare data in Saudi Arabia is almost three times higher than those in other countries in the survey (i.e., Australia, Brazil, England, Norway, Singapore, and the United States.)

⁴²³ *Id.* at 111.

⁴²⁴ Majid M. Altuwaijri, *The Impact of HealthCare Cybersecurity on Saudi Arabian Consumers*, ACCENTURE, at <https://www.accenture.com/sa-en/insight-accenture-health-2017-consumer-survey> (last visited Nov. 13, 2018).

▪ Data breach incidents and the legal response

Another way to assess the level of awareness is to observe the legal interactions that result after a privacy violation. Before listing the examples of the data breaches that have occurred in Saudi Arabia, it is important to note that Saudi Arabia does not have any law that requires organizations to report data breaches. Thus, the only way to know about the breach is through the media or if the organizations voluntarily notify their customers. What follows is a list of some of the data breach incidents that have occurred in Saudi Arabia:

- 1- In January 2012, the Hacker News published that the database of King Saud University (KSU) was exposed online to the public after a cyber-attack from unknown Hacker.⁴²⁵ The exposed data contained phone numbers, addresses, and passwords of 812 users. The passwords were not encrypted. No further news has been published about the identity of the hacker.
- 2- In August 2012, Aramco Company, the largest oil company in the world, experienced one of the biggest hacks in history. Nearly 35,000 computers were destroyed or partially wiped by a virus resulting in the deletion of data on the company's hard-drives. The company blamed foreign hackers for the attack.
- 3- In June 2013, Alyaum, a Saudi newspaper, published an investigation regarding the existence of anonymous marketing companies that offer databases including the names and telephone numbers of female teachers and employees for only 1500 Saudi Riyals.⁴²⁶ The sale of this information is aimed at women's concerns, clubs, sports clubs, private hospitals, beauty clinics, slimming and real estate marketing offices. Following the

⁴²⁵ *Saudi Arabia's King Saud University Database Hacked*, THE HACKER NEWS, Jan. 22, 2012 at <https://thehackernews.com/2012/01/saudi-arabias-king-saud-university.html>.

⁴²⁶ *Tasrib Bayanat 40 'alf muelimat Lisharikat Taswiq, [A Leak of Data of 40 Thousand Female Teachers to Marketing Companies]*, ALYAUM, Jun. 6, 2013, available at <http://www.alyaum.com/articles/876495/>.

investigation, one of the companies pursuing this method of violating the privacy of citizens reported that it had more than 1.5 million mobile numbers for citizens in Saudi Arabia's largest cities (i.e., Riyadh, Jeddah, and Dammam). There is no further news regarding the fate of these marketing companies. In fact, the online offers continue.

In April 2018, AlMowaten, a Saudi electronic newspaper, published a similar report about online offers of hundreds of thousands of Saudis' personal information at one of the most famous online stores in Saudi Arabia.⁴²⁷ The report indicated that the phone numbers were categorized according to age, gender, and sometimes other classifications such as a job to create targeted ads.⁴²⁸ Surprisingly, getting access to a vast database full of personal data is still an easy task. Many online websites offer these databases for small amounts (between 600 to 2000 Saudi Riyal).⁴²⁹ There has been no news about any legal action taken to stop the online offers of personal data.

- 4- In December 2016, many Saudi government websites were hacked; among these was the Saudi's General Authority of Civil Aviation.⁴³⁰ The Saudi news agency stated, "The attacks aimed at disabling all equipment and services that were being provided. The attackers were stealing data from the system and were planting viruses."⁴³¹ During the same month, a conference about the cybersecurity held at Taibah University announced that 200 governmental entities received about 680 hacking attempts. Moreover, according

⁴²⁷ Walid Alfahmi, *Bayanat Alsaediyyn fi khutr Tubae fi "Asiwaq Alnakhasat Al'iilktrunia" [Between 600 and 2000 rials you can get huge databases: Saudi data at risk .. Sold in "electronic markets"]*, ALMOWATEN, Apr. 18, 2018.

⁴²⁸ Walid Alfahmi, *bayanat almuatinin eabr al'intrnt [Citizens' information for sale online: Names and Addresses Indexed by Age and Gender]*, ALMOWATEN, Apr. 14, 2017.

⁴²⁹ *Id.*

⁴³⁰ Jose Pagliery, *Hackers Destroy Computers at Saudi Aviation Agency*, CNN, Dec. 2, 2016, available at <https://money.cnn.com/2016/12/01/technology/saudi-arabia-hack-shamoon/index.html>.

⁴³¹ *Id.*

to Kaspersky Lab, during a workshop in 2017, 60% of institutions in Saudi Arabia had experienced cyber-attacks over the prior 12 months.⁴³²

On the other hand, many successful cyber-attacks have been conducted by Saudi white hackers, who were trying to advise the government to develop more sophisticated cyber security systems to protect individuals' personal information. For example, a Saudi hacker known as "cyber of emotion" hacked more than 24 governmental websites in two hours. The hacker announced on his twitter account, "After the government websites ignored our messages about a possible attack, the group today announces that it is targeting poorly protected government sites and will tell you about the results"⁴³³

5- In April 2017, there was news that a cyber-attack hit STC, the largest telecommunications company in Saudi Arabia, and resulted in a data breach. However, the company denied the story through Sabq (Saudi newspaper), and it announced that the company would sue the source of this false news.⁴³⁴ In June 2018, Sabq reported that the police arrested the hacker who had hacked STC and leaked customers' information to the public. The news did not indicate when that cyber-attack occurred or how many consumers had been potentially harmed.

These cyber-attacks not only compromise people's information privacy, but they also cost the organizations considerable amounts of money. Although there were no sanctions or fines announced as a result of data breaches in Saudi Arabia, the cost of data breaches in Saudi Arabia

⁴³² Study: 60% of Saudi Institutions Hit by Virus Attacks, Malware, ARAB NEWS, Sep. 30, 2017, available at <http://www.arabnews.com/node/1169846/saudi-arabia>.

⁴³³ Hakar Saeudiun Yahkir 24 Mwqeaan Hkwmayaan Khilal Saeatayn [Saudi Hacker Penetrates 24 Government Sites Within Two Hours], AL RIYADH, Aug. 15, 2015, available at <http://www.alriyadh.com/1073358>.

⁴³⁴ Abdullah Albarqawi, *Alaitisalat Alsewdyt Tanfi Aikhtiraq Anzmtha: Almaelumat Almusribat Qadimh [STC denies penetration of its systems: leaked information is old]*, SABQ ONLINE NEWSPAPER, Apr. 5, 2017, at <https://sabq.org/DkcYJ8>.

and the United Arab Emirates is higher than in the rest of the world, according to tech giant IBM Security.⁴³⁵ On October 31, 2017, as a response to these massive numbers of cyber threats and data losses, Saudi Arabia took a step to establish a new authority on cybersecurity (i.e., National Cybersecurity Authority).⁴³⁶ NCA aims to protect the critical infrastructures and national security, according to Dr. Musaed Al-Aiban, who has been appointed as chairman of the board of directors of the authority.⁴³⁷ NCA has been granted the power to report to the King directly.⁴³⁸

➤ **Obstacle 7: The level of legal qualification for information privacy is weak**

Lawyers play a vital role in safeguarding people's private information by pursuing legal actions after data breaches occur. The legal battle will create more pressure on the organizations to protect individuals' personal information. The role of lawyers is even more significant if the level of supervisory authority is weak. In Saudi Arabia, there is no specific supervisory authority to be sure that the existing laws that protect individuals' information privacy are being enforced or to impose penalties on the violators. Thus, the existence of academics and lawyers specializing in information privacy laws is necessary in order to ensure that the legal provisions that protect people's rights to privacy are upheld.

Recently, Saudi Arabia began paying greater attention to cybersecurity. NCA signed an agreement with the Ministry of Education to grant 1,000 students the opportunity to study

⁴³⁵ MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY, REPORT: \$ 3.11 MLN COST OF DATA BREACH IN SAUDI ARABIA AND UAE, at <https://www.mcit.gov.sa/en/media-center/news/92153> (last visited Nov. 10, 2018).

⁴³⁶ *Saudi Arabia Sets up New Authority for Cyber Security*, REUTERS, Nov. 1, 2017, available at <https://www.reuters.com/article/us-saudi-cyber-security/saudi-arabia-sets-up-new-authority-for-cyber-security-idUSKBN1D13HS>.

⁴³⁷ *King Orders Setting up of National Cyber Security Authority*, SAUDI GAZETTE, Nov. 1, 2017, available at <http://saudigazette.com.sa/article/520782/SAUDI-ARABIA/King-orders-setting-up-of-National-Cyber-Security-Authority>.

⁴³⁸ *Id.*

cybersecurity and artificial intelligence during the next five years.⁴³⁹ Further, King Saud University officially announced that it would begin teaching cybersecurity as a new major starting next year.⁴⁴⁰ Additionally, there is some news about a new cybersecurity school that will be established in Riyadh within the next two years. This new movement that involves teaching cybersecurity is a significant step forward aimed at protecting individuals' personal information.

However, most of the attention given to information is rooted in technology. There are more than 40 universities in Saudi Arabia, and none of these universities teaches information privacy laws. As a result, studies and articles on information privacy in Saudi Arabia are rare. Most academic papers approach information privacy from a technological perspective. For example, both of the studies mentioned previously in this dissertation that served to measure the level of privacy awareness in Saudi Arabia were written by people specialized in Computing and Information Sciences.

After all, teaching information privacy at Computing and Information Sciences schools is necessary in order to work on reducing the chances that people's private information will be illegally disclosed; these schools are responsible for a proactive approach. Nevertheless, teaching information privacy at the law schools is equally important because keeping personal information fully secured and protected from any illegal use or disclosure is probably impossible. Thus, having law graduates who are specialized in information privacy laws will help in locating the gaps in the current rules, developing new regulations, and assisting people in receiving increased levels of privacy protection, as promised by the Saudi constitution and Sharia.

⁴³⁹ Abdullah Albarqawi, *Altaqdim Aalaa Alaibtieath fi Tkhssat Al'amn Alsibrany Ghdaan* [Applying for Scholarships in Cyber Security Starts Tomorrow], SABQ ONLINE NEWSPAPER, Jun. 23, 2018, at <https://sabq.org/Vx8TKH>.

⁴⁴⁰ Fahad Algabywi, *Jamieat Almalik Sueud Tutrah 3 Tukhasusat Jadidatan Ibkawryws Alttalibat* [King Saud University Offers 3 New Specializations for Female Students], SABQ ONLINE NEWSPAPER, Jun. 16, 2018, at <https://sabq.org/JLD94y>.

❖ Conclusion

Leading up to this chapter, the author had described the legal protection guaranteed to Saudi citizens, via both Sharia principles and Saudi legislation, with regard to their private information. In this chapter, the author pointed out the practical obstacles that serve to influence the level of privacy protection citizens are actually guaranteed. Among these obstacles is Saudi Arabia's lack of specific data protection law; as the country has multiple laws that are not designed primarily to protect privacy, it is difficult to know which court among the six might best serve to protect citizens' information privacy. Further, the multiplicity of courts that are entitled to hear cases concerning the protection of individuals' personal data has made it more difficult to predict a court's decision since each of one these courts might be guided via different principles. An example of this involves the difference between the General Sharia Courts and the Board of Grievances regarding compensation for moral damage, which is a critical issue for receiving compensation for privacy violations.

Moreover, it is vital that some general Sharia principles are used to protect individuals' privacy for an extended period, yet all of these principles came to be a long time before the technological revolution and thus do not take into account issues related to technology. Sharia requires judges to meet certain qualifications before they can apply the old principles to new issues (practicing *ijtihad*). However, most Saudi judges are not qualified to practice *ijtihad*. This keeps these principles from being applied and from potentially addressing novel issues associated with technology. Further, even if a judge decides a case after diligent work, other judges in similar or lower courts are not legally bound by the precedent. Moreover, another obstacle is rooted in Saudi Arabia's legal system in that the legal system does not recognize class

action cases, which increase the chances that people whose personal information has been violated will sue the offending organization for the damages, which are usually moral in nature.

Lastly, Saudi citizens value their rights to privacy, but they tend to be unaware of the ways in which their privacy maybe violated, and they are especially unaware of the violations that result from technology. Unlike the computing and informatics science schools, law schools in Saudi Arabia have yet to recognize the importance of teaching information privacy law, and this serves to further indicate the low level of awareness regarding the ways in which technology can result in citizens' privacy rights being violated. In addition, this means that legal reaction to violations is often weak and insufficient. The next chapter proposes means of increasing the level of information privacy protection afforded to citizens in Saudi Arabia.

Chapter 4: The future of information privacy in Saudi Arabia

❖ Introduction

After discussing Saudi Arabia's level of information privacy protection and pointing out the primary obstacles and flaws regarding the current information privacy framework, this chapter offers an overview of the key steps that must be taken if the legal protection provided to safeguard citizens' personal information is to be improved. It is worth noting, however, that there is no perfect solution that will address all privacy issues, especially given how rapidly technology is changing.

Most countries around the world, including the United States and the European countries, approach information privacy protection differently. These countries are trying to find the best way to protect people's rights to privacy without hindering business. For example, in the United States, there is no comprehensive federal data protection law that aims to protect all personal data; instead, the U.S. has several federal and state laws and regulations that serve this end. Each of these laws and regulations aims to protect people's private information differently. The Health Insurance Portability and Accountability Act, for instance, focuses on the protection of individuals' health information, while the Fair Credit Reporting Act governs personal information assembled by Credit Reporting Agencies.

The European Union, however, chose another approach by which to protect personal data; in 2016, it introduced what is arguably the most sophisticated data protection law (General Data Protection Regulation, "GDPR"), and this law was implemented in May 2018. The GDPR is a comprehensive data protection law that governs the collection, use, and disclosure of personal data in both the public and private sectors. Like the United States and the European Union, Saudi Arabia will have to find its own best way to protect citizens' private information,

and it will have to do this by taking advantage of the extant information privacy systems employed in other countries.

Before diving into the recommended steps to this end, it might be worth illustrating why it is necessary for Saudi Arabia to move ahead in order to protect information privacy and increase people's privacy protections.

A. Why does Saudi Arabia need to improve on its information privacy protections?

1- To meet the level of protection granted via Sharia law in an era characterized by technological advances.

The Saudi Constitution guarantees human rights protected by Sharia law, and one of the most important human rights is the right to privacy. The Saudi Constitution explicitly offers protection of the privacy of homes and personal communications. However, today, thanks to technology, people's private information is used and extends beyond homes and personal communications, and some of this information might reveal more than what a phone call could disclose. Thus, protecting citizens' rights to privacy needs to involve more than just safeguarding individuals' homes and personal communications. The previous chapter explained the obstacles and flaws associated with the Saudi information privacy framework that serve to limit or weaken the level of legal protection of individuals' personal information provided by both Sharia law and Saudi regulation. Improving the extant legal protection of information privacy is essential to meeting the level of protection granted via Sharia law in the currently technology-advanced era.

2- Technology plays a vital role in the future of Saudi Arabia.

In 2016, the Crown Prince Mohammed bin Salman launched Saudi Vision 2030, which is a long-term plan to diversify the Saudi economy and reduce the country's reliance on oil.⁴⁴¹ One of the primary goals of Saudi Vision has to do with technology.⁴⁴²

a. Developing a digital infrastructure

Saudi Vision 2030 recognizes that a sophisticated digital infrastructure is a keystone of today's advanced industrial activities, as it can attract investors and enhance an economy's competitiveness.⁴⁴³ Thus, Saudi's government is planning to partner with the private sector in order to improve the telecommunications and information technology infrastructures.⁴⁴⁴ One of the primary goals is to expand high-speed broadband coverage such that it reaches 90% of cities.⁴⁴⁵ The plan includes the support of local investment in the telecommunications and information technology sectors so that technological growth can occur. Meanwhile, the legislative authorities have been tasked with making improvements to the current regulations to help the government in establishing an active partnership with telecommunications companies and further developing the business environment.⁴⁴⁶

b. Leader in E-government

Moreover, another means by which technology is being used to achieve the objectives of the Kingdom's Vision 2030 involves the expansion of the scope and quality of online government services, as this will permit the country to become a global leader in e-government

⁴⁴¹ THE OFFICIAL WEBSITE OF THE SAUDI VISION 2030, at <http://vision2030.gov.sa/en>.

⁴⁴² SAUDI VISION 2030, A DEVELOPED DIGITAL INFRASTRUCTURE, at <http://vision2030.gov.sa/en/node/97> (last visited Nov. 10, 2018).

⁴⁴³ *Id.*

⁴⁴⁴ *Id.*

⁴⁴⁵ *Id.*

⁴⁴⁶ *Id.*

transactions.⁴⁴⁷ According to a UN e-government survey, Saudi Arabia's ranking jumped from 90 in 2014 to 36 in 2014.⁴⁴⁸ Progress has been made regarding many e-government services, including "employment programs, online job searches, e-learning services, traffic, passports and civil affairs, online payment services, online issuance of commercial registers, among others."⁴⁴⁹ The Saudi government announced a goal to raise Saudi's ranking by 2030 on the E-government Survey Index so that it can be among the top five countries.⁴⁵⁰ The government is aiming to expand the scope of its current e-government services to include additional areas such as education and healthcare.⁴⁵¹ Further, Saudi Vision 2030 encourages government agencies to use online applications such as cloud applications, data sharing platforms, and HR management systems.⁴⁵²

c. Building "Smart Cities"

The Saudi government announced its intention to partner with the private sector to build "Smart Cities." In 2017, Riyadh held the first Smart Cities annual conference with over 700 participants from ministries and governmental bodies from across the county in attendance.⁴⁵³ The Ministry of Municipal and Rural Affairs led the conference to initiate discussion regarding finding or establishing the best practices and leading technologies and services that might help to

⁴⁴⁷ SAUDI VISION 2030, EFFECTIVE E-GOVERNMENT, at <http://vision2030.gov.sa/en/node/13> (last visited Nov. 10, 2018).

⁴⁴⁸ UNITED NATIONS, GLOBAL E-GOVERNMENT READINESS REPORT (2004), available at <https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2004-Survey/Complete-Survey.pdf>; Also, UNITED NATIONS, GLOBAL E-GOVERNMENT SURVEY (2014), available at https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf.

⁴⁴⁹ Saudi Vision 2030, *supra* note 447.

⁴⁵⁰ *Id.*

⁴⁵¹ *Id.*

⁴⁵² *Id.*

⁴⁵³ Saudi Smart Cities, at <https://www.saudismartcities.net/>.

provide foundation for the upcoming Smart Cities.⁴⁵⁴ It has been reported that the Saudi government will be investing over \$500 billion to modernize its infrastructure across the 285 municipalities in order to provide the best quality of life for its people.⁴⁵⁵

Further, in October 2017, the Saudi Crown Prince Mohammed bin Salman revealed the Kingdom's ambitious project to build a smart megacity called "NEOM" from scratch.⁴⁵⁶ The plan is to build this huge city, which will take up to 26,500 square kilometers of land, as a high-tech zone that will incorporate artificial intelligence and the Internet of Things.⁴⁵⁷ Prince Mohammed described some features of NEOM in an interview with Bloomberg; he stated, "Your medical file will be connected with your home supply, with your car, linked to your family, linked to your other files." He also noted that the "system develops itself in how to provide you with better things."⁴⁵⁸ Prince Mohammed is picturing an app-driven city that is almost entirely automated and responsive to the needs of its residents. The Saudi government has set other highly ambitious goals regarding NEOM; for example, the city is to run on wind and solar energy, making the numbers of robots more than humans.⁴⁵⁹ The initial operations will

⁴⁵⁴ *Id.*

⁴⁵⁵ *Id.*

⁴⁵⁶ Samia Nakhoul & Stephen Kalin, *New Saudi Mega-city is Prince's Desert Dream*, REUTERS, Oct. 27, 2017, available at <https://www.reuters.com/article/us-saudi-economy-vision-analysis/new-saudi-mega-city-is-princes-desert-dream-idUSKBN1CW2G6>.

⁴⁵⁷ Katie Pyzyk, *Saudi Arabia Announces \$ 500B Plan to Build a New Megacity*, SMART CITIES DRIVE, Oct. 30, 2017, at <https://www.smartcitiesdrive.com/news/saudi-arabia-announces-500b-plan-to-build-a-new-megacity/508388/>.

⁴⁵⁸ Alaa Shahine, Erik Schatzker, Vivian Nereim, & Glen Carey, *Saudis Are Talking to Amazon, Alibaba About New City, Prince Says*, BLOOMBERG, Oct. 26, 2017, available at <https://www.bloomberg.com/news/articles/2017-10-26/saudis-are-talking-to-amazon-alibaba-over-new-city-prince-says>.

⁴⁵⁹ Vivian Nereim, Glen Carey & Christopher Cannon, *Sun, Sea and Robots: Saudi Arabia's Sci-Fi City in the Desert*, BLOOMBERG, Oct. 26, 2017, available at <https://www.bloomberg.com/graphics/2017-neom-saudi-mega-city/>.

begin in the last quarter of 2019, and the city is expected to open for business in its first phase in 2025.⁴⁶⁰

d. E-commerce in the retail sector

When creating Saudi Vision 2030, the Saudi government noticed that traditional retail outlets control 50% of the country's market compared to the 20% market share it controls in other countries in the Gulf Cooperation Council (GCC).⁴⁶¹ The government also noted that the retail market suffers from a lack of modern commerce and e-commerce. Thus, the government wishes to increase contemporary trade and e-commerce to 80% of the retail sector by 2030.⁴⁶² The plan is to achieve the goal by "attracting both regional and international retail investors and by easing restrictions on ownership and foreign investment."⁴⁶³

e. Investing in emerging technologies

To help diversify the Kingdom's economy, the 2030 Vision introduced the idea of privatization of state-owned assets, including leading companies such as ARAMCO to bring more diverse revenues for the Saudi government.⁴⁶⁴ This will further enhance the government's financial resources and increase the government's ability to invest in large international companies and emerging technologies from around the world.⁴⁶⁵

Therefore, achieving the Saudi Vision technological goals, which include the construction of Smart Cities, improving the telecommunications and information technology

⁴⁶⁰ *Id.*

⁴⁶¹ SAUDI VISION 2030, OUR COMMITMENTS , at <http://vision2030.gov.sa/en/commitments> (last visited Nov. 10, 2018).

⁴⁶² *Id.*

⁴⁶³ *Id.*

⁴⁶⁴ SAUDI VISION 2030, MAXIMIZING OUR INVESTMENT CAPABILITIES, at <http://vision2030.gov.sa/en/node/82> (last visited Nov. 10, 2018).

⁴⁶⁵ *Id.*

infrastructures, and expanding the government's online services, requires the Saudi government to induce both local and international private sectors to invest in the Saudi market. The Crown Prince announced that the Saudi government has begun talking with companies such as Amazon and Alibaba about what technology options they could bring to the app-driven city.⁴⁶⁶ In addition, NEOM's Chief Executive Klaus Kleinfeld states, "We've had a huge amount of interest, and we're talking to a lot of companies that are at the forefront of technologies wanting to partner with us and try out things in NEOM. On the technological side, a lot of people look at it as a place where they think they can try a lot of things out."⁴⁶⁷

Recently, the Crown Prince visited the Silicon Valley and Seattle to meet with top executives from Amazon, Microsoft, Apple, Google, and other big tech companies to discuss the new business opportunities in the Saudi market.⁴⁶⁸ The results of those meetings have already begun to materialize. According to Reuters, Apple and Amazon have already begun talking with the Saudi government regarding licensing and investment in Saudi Arabia.⁴⁶⁹ Both companies already sell their products in Saudi Arabia via third parties because of the legal restrictions on foreign ownership. During the last year, the Saudi government has been easing regulatory impediments in order to bring foreign investors to the Saudi market.⁴⁷⁰ Therefore, Apple, Amazon, and other big international high-tech companies will be able to establish a direct

⁴⁶⁶ Alaa Shahine, Erik Schatzker, Vivian Nereim, & Glen Carey, *supra* note 458.

⁴⁶⁷ Holly Ellyatt, *Saudi's \$500 billion Mega-city NEOM is Attracting 'Overwhelming' Interest from Investors*, CNBC, May. 10, 2018, at <https://www.cnbc.com/2018/05/10/saudis-500-billion-mega-city-neom-is-attracting-overwhelming-interest-from-investors.html>.

⁴⁶⁸ Margherita Stancati & Ben Fritz, *Saudis Want Fewer Weapons, More Disney in U.S. Business Talks*, THE WALL STREET JOURNAL, Apr. 5, 2018, available at <https://www.wsj.com/articles/saudis-want-fewer-weapons-more-disney-in-u-s-business-talks-1522931617>.

⁴⁶⁹ Katie Paul, *Exclusive: Apple and Amazon in Talks to Set up in Saudi Arabia*, REUTERS, DEC. 28, 2017, available at <https://www.reuters.com/article/us-saudi-tech-exclusive/exclusive-apple-and-amazon-in-talks-to-set-up-in-saudi-arabia-sources-idUSKBN1EM0PZ>.

⁴⁷⁰ *Id.*

presence in the Saudi market. For example, Apple's first retail store in the country is expected to open in 2019.⁴⁷¹ Additionally, Google has already signed a cloud-computing contract with Saudi Arabia,⁴⁷² and Amazon has spoken with the Saudi government about the possibility of bringing the cloud-computing division Amazon Web Services (AWS) to Saudi Arabia.⁴⁷³

To induce international companies to invest in the Saudi market, the government is working hard to improve its business environment and ranking on the World Bank's "ease of doing business index."⁴⁷⁴ According to Ibrahim Al-Omar, governor of the Saudi Arabian General Investment Authority (SAGIA), the goal is rank 20th (today Saudi Arabia ranks 92nd).⁴⁷⁵ To further entice foreign investors, the crown prince has explained that NEOM will operate independently of the rest of the government, and it will thus have its own tax laws, labor laws, and judicial system. It would be, in effect, a "free zone."⁴⁷⁶

The framework and facilities established to entice foreign investors rely heavily on Saudi Arabia's lawmakers and judicial system. Given the country's significant advances regarding technology, as well as the Saudi government's considerable efforts aimed at luring high-tech companies from around the world to invest in the Saudi market, it is worth noting that the regulations and Sharia principles that govern individuals' personal information continue to use broad language, and the courts' decisions regarding privacy violation are thus difficult to predict.

⁴⁷¹ Katie Paul, *Apple and Amazon in Talks to Set up in Saudi Arabia*, CNBC, DEC. 28, 2017, available at <https://www.cnbc.com/2017/12/28/apple-and-amazon-in-saudi-arabia-talks-sources.html>.

⁴⁷² Mark Bergen, *Google, Thiel Feature in Saudi Prince's Silicon Valley Tour*, BLOOMBERG, Apr. 6, 2018, available at <https://www.bloomberg.com/news/articles/2018-04-06/google-thiel-stand-out-in-saudi-prince-s-silicon-valley-tour>.

⁴⁷³ Olivia Zaleski & Spencer Soper, *Amazon Makes Hiring Push in Riyadh After Saudi Prince's Visit*, BLOOMBERG, Apr. 5, 2018, available at <https://www.bloomberg.com/news/articles/2018-04-05/amazon-makes-hiring-push-in-riyadh-after-saudi-prince-s-visit>.

⁴⁷⁴ Holly Ellyatt, *supra* note 467.

⁴⁷⁵ *Id.*

⁴⁷⁶ Katie Pyzyk, *supra* note 457.

Vague rules, such as these, increase the risk of a tech company unknowingly conducting unlawful actions when handling private information in Saudi Arabia, and this is especially true when the company is a foreign entity less familiar or unfamiliar with Sharia principles. Furthermore, the expansion of the technology market in Saudi Arabia means an increase in the volume of individuals' personal information that is created, used, and exchanged, and it is increasingly likely that foreign companies will collect, store, and perhaps transfer much of this information.

It is thus important to establish new, well-defined rules that will protect people's private information and that will benefit not only the people of Saudi Arabia but also Saudi's emerging technology market. Having a clearly defined information privacy system will help to reduce risks for foreign tech companies wishing to enter the Saudi market, and this will eventually encourage more companies to invest greater amounts more quickly. Clearer laws, which will be more accessible, will also enhance the protections afforded to individuals regarding their rights to privacy. The ambiguous nature of extant laws serves to keep individuals from becoming familiar with their present rights and, therefore, from pursuing them.

Unfortunately, there is no a perfect information privacy law that Saudi Arabia might directly adopt that will solve all of the country's privacy issues, especially the issues related to the use of technology. Different countries approach information privacy issues differently, in ways that best suit them. Countries around the world use several models to protecting people's personal information: comprehensive, sectoral, self-regulatory, and co-regulatory models. Many of these countries employ a combination of these models. As such, Saudi Arabia will have to find its own means of protecting information privacy and creating a stable market in order to both safeguard individuals' privacy as a human right and reduce risks faced by foreign

technology companies. This dissertation does not compare in detail the different models used in effort to find the best model to adopt in Saudi Arabia. This chapter, however, will provide a brief definition of each model, discuss the possibility of adopting a comprehensive data protection law similar to the European GDPR in Saudi Arabia, and assess the advantages and disadvantages of adopting such a law.

B. Recommendations for protecting information privacy in Saudi Arabia

1- Adopting a formal law

The number of countries that have developed information privacy protection rules has snowballed in recent years. According to United Nations Conference on Trade and Development (UNCTAD) surveys, 108 countries have already implemented formal laws either a comprehensive or partial data protection laws.⁴⁷⁷ The survey also shows that roughly 30% of the countries around the world have no data protection laws in place.⁴⁷⁸ The states without data protection laws suffer from reduced trust and confidence as they pertain to an array of commercial activities. Additionally, these countries are losing out on many international trade opportunities because many trade-related transactions involve cross-border data transfers that require minimum legal protections.⁴⁷⁹ Meeting these cross-border data transfers requirements is a difficult task in the absence of data protection legislation. Thus, more than 35 countries are currently drafting data protection laws so that they might overcome these issues.⁴⁸⁰ Countries around the world use different forms of formal laws to protect individual's privacy. Also, some of these countries apply more than one form of formal laws.

⁴⁷⁷ UNITED NATION CONFERENCE ON TRADE AND DEVELOPMENT, DATA PROTECTION REGULATIONS AND INTERNATIONAL DATA FLOWS: IMPLICATIONS FOR TRADE AND DEVELOPMENT (2016), available at http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

⁴⁷⁸ *Id.* at 8.

⁴⁷⁹ *Id.*

⁴⁸⁰ *Id.*

a. Comprehensive law

Many countries around the world have adopted comprehensive data protection laws that govern the collection, use, and dissemination of personal information by both the public and private sectors.⁴⁸¹ This is the preferred model for most countries, especially in Europe.

According to UNCTAD's Cyberlaw Tracker, as of April 2016, 108 countries had implemented national data protection laws.⁴⁸² The laws are all somewhat different, but they have the same purpose, which is to regulate the collection, use, and disclosure of personal information. Ninety-five of the laws are specific comprehensive data protection laws.⁴⁸³ Most of these countries have an official or agency that oversees and enforces the data protection laws.⁴⁸⁴ The duty of this official, known as a Commissioner, Ombudsman, or Registrar, is to oversee compliance with the law and to investigate any alleged breaches.⁴⁸⁵

There are many reasons why most countries prefer adopting a comprehensive law to protect personal information, such as promoting e-commerce and ensuring consistency with EU laws. Many countries have established well-defined comprehensive data protection laws to promote electronic commerce, as these laws help to ensure that the personal information of consumers around the world is protected.⁴⁸⁶ Moreover, given the adequacy requirement of the EU Directive and the current GDPR, many countries are adopting comprehensive laws to ensure

⁴⁸¹ David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection and Surveillance Law and Developments*, 18 J. Marshall J Computer & Info L. 1 (1999).

⁴⁸² UNITED NATION CONFERENCE ON TRADE AND DEVELOPMENT, DATA PROTECTION REGULATIONS AND INTERNATIONAL DATA FLOWS: IMPLICATIONS FOR TRADE AND DEVELOPMENT (2016), available at http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

⁴⁸³ *Id.*

⁴⁸⁴ David Banisar & Simon Davies, *supra* 481.

⁴⁸⁵ *Id.*

⁴⁸⁶ *Id.*

that the requirements of the EU data protection laws will not affect trade.⁴⁸⁷ Lastly, usually, the comprehensive data protection law has fewer exceptions and makes individuals' privacy rights the primary priority.

b. Sectoral laws

Some countries, even countries that have general data protection laws, offer protection of people's personal information via the implementation of several laws that address specific industry sectors, such as laws pertinent to financial privacy and health information privacy.⁴⁸⁸ Sectoral laws usually offer full protection for specific categories of information such as telecommunications, police files, and consumer credit records.⁴⁸⁹ Having several laws, however, might allow for either a gap or an area of overlap between or among the laws, and keeping all of these laws updated so that they remain relevant in the face of new technology is difficult.⁴⁹⁰ the sectoral laws exist in many countries around the world, even in countries that have general data protection laws such as Canada, and Australia.⁴⁹¹

Most of the countries that use sectoral data protection laws have established these laws over the course of many years. For example, in the United States, the Freedom of Information Act was enacted in 1966, the Fair Credit Reporting Act was enacted in 1970, the Privacy Act

⁴⁸⁷ *Id.* See also Tiffany Curtiss, *Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies*, 12 WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS 95 (2016).

⁴⁸⁸ For example, see Health Insurance Portability and Accountability Act, and Fair Credit Reporting Act.

⁴⁸⁹ Curtiss, *supra* note 487 at 14.

⁴⁹⁰ David Banisar & Simon Davies, *supra* 481. See also Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TECH PRIVACY, Nov. 13, 2015, at <https://teachprivacy.com/problems-sectoral-approach-privacy-law/>.

⁴⁹¹ For example, in Australia, the health sector in New South Wales and Victoria is regulated by the Health Record and Information Privacy Act (2002). Also, in Canada, in the health sector, there are several provincial statutes may apply in addition to, or in place of the Personal Information Protection and Electronic Documents Act (*PIPEDA*).

was implemented in 1974, the Health Insurance Portability and Accountability Act was enacted in 1996, the Children's Online Privacy Protection Act was enacted in 1998, and the Gramm-Leach-Bliley Act was enacted in 1999. Thus, establishing numerous laws intended to regulate different industries may prove challenging for Saudi Arabia, as the laws created could result in either gaps or overlaps in protection.

c. Other forms of formal laws

Countries can also protect individuals' personal information by utilizing an existing general law that it is not a comprehensive data protection law or a sectoral law targeting any specific industry. An example of this is the protection of information privacy offered by the Federal Trade Commission's general authority under section 5 of the Federal Trade Commission (FTC) Act. Section 5 of the FTC Act allows the FTC to investigate "unfair and deceptive acts and practices in or affecting commerce." The FTC has used this general authority to protect individuals' privacy by ensuring that companies adhere to their own stated policies. The FTC finds those companies that elect not to adhere to their own stated policies to be engaging in deceptive acts or practices.⁴⁹² The FTC also has authority to enforce several sectoral laws such as the Children's Online Privacy Protection Act and the Fair Credit Reporting Act.⁴⁹³

➤ **Adopting a comprehensive data protection (GDPR-like) law is the best long-term goal for Saudi Arabia**

On May 25, 2018, the European General Data Protection Regulation (GDPR) became enforceable, replacing the 1995 Data Protection Directive. The GDPR is taking a step forward to strengthen the third-party's obligations and offering legal protection of personal data belonging

⁴⁹² FEDERAL TRADE COMMISSION, PRIVACY AND DATA SECURITY UPDATE (2016), *available at* <https://www.ftc.gov/reports/privacy-data-security-update-2016>.

⁴⁹³ *Id.*

to EU citizens even when they are outside EU countries. Additionally, the GDPR requires that personal data can only be transferred outside of the European Economic Area (EEA) in limited: 1) if the European Commission finds that a third country or specific sector within the third country is offering “adequate level of protection”; 2) the data controller or data processor provides appropriate protection; and 3) the data subject has provided explicit consent to the transfer.⁴⁹⁴ By strengthening third-party obligations and the sanctions reaching non-EU countries, GDPR is exporting its privacy norms to countries and companies around the world. There would be many advantages associated with the adoption of a clear and comprehensive (GDPR-like) law in Saudi Arabia, but there would also likely be a number of challenges that would make adoption of this sort of law difficult presently.

- **The advantages of adopting a comprehensive data protection law in Saudi Arabia**

Unlike the other models, the primary benefit of issuing a comprehensive data protection law is that the law will be the product of lawmakers who usually place public interest ahead of private interest, and the government will be responsible for overseeing enforcement of the legislation. In Saudi Arabia, right to privacy is being promised as a fundamental human right guaranteed by Sharia principles and the Saudi constitution. However, the absence of a clear law whose aim is primarily to protect individuals’ personal information in the digital age results in inadequate privacy protection. Trusting the companies to go against their interests as they pertain to the use of people's personal information as well as to deliver a high level of protection in absence of a comprehensive law with which they must comply is unrealistic.

⁴⁹⁴ Article 44-55 Of General Data Protection Regulation.

Moreover, having a clear and well-defined data protection law will reduce risks for both local and international companies seeking to invest in Saudi Arabia. Even though the new law will demand more of companies that deal with personal information, it will be easier for those companies to identify the legal requirements and assess potential risks. Currently, the laws and the Sharia principles that serve to protect individuals' private information tend to use a broad language, which has resulted in a state of uncertainty that increases the possibility that a company might unintentionally violate some of the privacy rules.

Likewise, by adopting a GDPR-like law, Saudi Arabia could become an approved third-party nation for international data transfer under the rules of GDPR. Being recognized by the EU Commission as a nation with "adequate level of data protection" will increase and perhaps accelerate the interest foreign tech companies have in entering the Saudi market, and this will serve the goal of Saudi Vision 2030 to create an attractive environment for high tech companies. The companies will be able to transfer personal data (subject to GDPR) from or to Saudi Arabia without worrying about adopting binding corporate rules (BCR) or signing standard contractual clauses to meet the requirements of the EU data protection laws.

An additional advantage of the comprehensive law model is that such a law would govern personal information in the both the private and public sectors. Many data breaches that have occurred in Saudi Arabia were the result of an inadequate level of data protection among government entities.⁴⁹⁵ Having a comprehensive law will push both private and public sectors to take more precautions to keep individuals' private information safe.

- **The challenges of adopting a comprehensive data protection law in Saudi Arabia**
 - **The high cost for both the government and the private sector**

⁴⁹⁵ See examples in the third chapter.

It is true that enacting a comprehensive data protection law has many advantages, but it also has its critics and difficulties, especially when it comes to developing countries such as Saudi Arabia. In many ways, the cost of enacting a comprehensive data protection law is high for both the government and private sectors. Starting with the cost to implement and enforce the law, the government will need to fund the enforcing body and address costs related to costly paperwork, documentation, auditing, and other requirements.⁴⁹⁶ Additionally, all of the government entities that will be subject to the law will bear the costs associated with cyber liability insurance as well as the costs associated with the tools and work necessary to ensure compliance with the law's requirements, such as the cross-border transfer.⁴⁹⁷ This is in addition to the possibility of paying compensations to harmed persons in the event that rules are violated that cause a person or persons harm.

Cost burdens would also affect all companies subject to the data protection law. For example, as a requirement of GDPR, companies would be required to appoint a representative to respond to privacy requests and conduct self-assessments. These costs do not take into account those associated with the hiring of skilled technicians to maintain information security in the first place.⁴⁹⁸ If costs related to a clear and comprehensive law are too high, then some foreign investors may be less interested in the Saudi market, as there are some companies that might prefer to take risks in a less financial burdensome market and legal system characterized by unclear data protection rules.

⁴⁹⁶ Curtiss, *supra* note 487 at 104.

⁴⁹⁷ See DATA PRIVACY SURVEY: GDPR COSTS AND COMPLEXITY A CONCERN, BARKER MAKENZIE, May. 4, 2016, available at <http://www.bakermckenzie.com/en/newsroom/2016/05/data-privacy-survey-gdpr-costs-and-complexity>.

⁴⁹⁸ Curtiss, *supra* note 487 at 104.

- **The lack of technicians specialized in information security and privacy professionals**

Another challenge facing Saudi Arabia and other developing countries looking to adopt a comprehensive data protection law is the lack of technicians specialized in information security and privacy professionals.⁴⁹⁹ This challenge is usually a result of a lack of local technical education opportunities.⁵⁰⁰ As mentioned in the previous chapter, Saudi Arabia recently began paying greater attention to cybersecurity, which led it to establish the National Cybersecurity Authority (NCA). The country also granted 1,000 students the opportunity to study cybersecurity abroad over the next five years, and it began ensuring that cybersecurity was offered as a new major course of study in several local universities. This attention to education as it relates to cybersecurity could be indicative of the country's shortage of technicians specialized in information security. The results of this movement will not be realized in the market for several years. And with regard to information privacy, Saudi Arabia has continued to neglect to give much attention to privacy protections professionals. There are more than 40 universities in Saudi Arabia, and none of these universities teaches information privacy law. In contrast, even developed countries, such as the United States, which has a long history related to its development of a data protection community and whose training and certification organizations have sought to meet the market need, have too few privacy protections professionals. For instance, the International Association of Privacy Professionals was established in 2000, and today just over 3,100 individuals currently are Certified Information Privacy Professional in the United States.⁵⁰¹

⁴⁹⁹ *Id.* at 109.

⁵⁰⁰ *Id.*

⁵⁰¹ *Id.*

Adopting a GDPR-like law requires numerous qualified individuals in both technology and privacy. This is necessary even for a law to be drafted, as the legislative authority will need specialists to draft a suitable data protection law locally and globally. Additionally, the data protection authorities will have to understand how companies' technologies work to avoid arbitrary determination.⁵⁰² Under a comprehensive model, every organization that collects personal information, including employee data, would have to comply with the law, and professionals would be necessary to make sure this happens. It would be challenging for both governmental and private organizations to apply the law without having a strong educational system that can keep pace with the market's need. The companies will not be able to find the necessary talent to help ensure that they comply with the law. As a result, such companies will be forced to bring in foreign employees, who would cost more, or they might choose to avoid the market entirely. The Labor Ministry recently introduced a new policy aimed at reducing the number of foreign employees in Saudi Arabia, so this could be problematic for companies in need of outside assistance.⁵⁰³

It is an obvious risk to adopt a comprehensive data protection law in Saudi Arabia before finding a solution that addresses insufficient talent capable of meeting the market's needs. Increased efforts to teach technological education is useful, but they are insufficient. As such, it is essential that the government work on additional ways to produce privacy professionals. This step has to be taken first by the government since there is no data protection law which would motivate educational institutions and organizations to teach information privacy.

⁵⁰² *Id.* at 111

⁵⁰³ Matthew Kalman , *Saudi Arabia: Labor Reforms Gather Pace as Government Seeks to Normalize Economy*, BLOOMBERG, Oct. 2, 2017, at <https://www.bna.com/saudi-arabia-labor-n73014470794/>.

- **Unsophisticated judicial regimes**

To be approved as a nation with an adequate level of protection under GDPR, data subjects would need meaningful access to remedies when privacy violations occur. For example, one of the main reasons behind the invalidation of the US-EU Safe Harbor agreement was insufficient access to the court under U.S. law.⁵⁰⁴ In Saudi Arabia, multiple courts have jurisdictions over privacy violations. The judges of these courts have different educational backgrounds; some hold only Sharia law degrees, while others hold law degrees. Further, the courts have different opinions on some critical issues related to privacy violations. For instance, the General Sharia Courts and the administrative courts have different opinions regarding the eligibility of a morally harmed person for compensations. There are not enough published privacy violations cases to compare the courts' decisions in these cases and measure the consistency. Thus, applying a GDPR-like law might not be enough to convince the EU Commission that Saudi Arabia should be an approved nation. With the current legal regime, Saudi Arabia is likely to find it difficult to meet the juridical requirements.

A comprehensive model is probably the best means by which Saudi Arabia can protect people's personal information as one of their fundamental rights and make the Saudi market a desirable market for foreign companies, as it will reduce companies' risks. In addition, a comprehensive model is probably the best route to ensure that Saudi Arabia is an approved third-party country for data transfer under the GDPR requirement. Nevertheless, adopting a comprehensive data protection law before first developing the foundations that make the law effectively applicable could backfire on the government and local and foreign companies. A lack

⁵⁰⁴ See Natasha Lomas, *Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement With U.S.*, TECHCRUNCH, Oct. 6, 2015, available at <https://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s/>.

of technical sophistication, privacy professionals, and effective courts make the immediate adoption of a GDPR-like law a risky choice. Solving the issues at hand might take a considerable amount of time, which means that it could be quite a while before the country is ready to adopt such a law. For example, to train and teach enough people to carry out the requirements of a comprehensive law within both governmental institutions and private companies will take several years. This does not mean that Saudi Arabia shall wait for years to improve upon its level of data protection. In fact, in the meantime, the country can employ a co-regulatory approach as an intermediate step toward the comprehensive model.

2- Adopting the co-regulatory approach as an intermediate step toward a comprehensive model

Individuals' personal information can be protected through several forms of self-regulation via which companies and industry bodies establish codes of practice.⁵⁰⁵ Many developed countries, even countries that have formal laws, use this approach to regulate certain industries. For example, in the United States, a self-regulatory program that addresses online behavioral advertising governs the advertising industry. The main advantages of self-regulation include efficiency, flexibility, an incentive for compliance, and reduced government costs,⁵⁰⁶ as self-regulation lowers the costs and burdens associated with data protection regulation for the government.⁵⁰⁷ Additionally, this approach can be effective when it comes to predicting future technologies and establishing standards that can accommodate change.⁵⁰⁸ However, adequacy and enforcement are major issues when it comes to self-regulation. Standards made by a given

⁵⁰⁵ *Id.* at 14

⁵⁰⁶ Bert-Jaap Koops, Miriam Lips, Sjaak Nouwt, Corien Prins & Maurice Schellekens, *Should Self-Regulation be the Starting Point?*, (IT & Law; No. 9). The Hague: T.M.C. Asser Press 109, 123-130 (2006).

⁵⁰⁷ *Id.*

⁵⁰⁸ *Id.*

industry could be weak and too lenient because industry representatives might be more inclined to look out for industry interests rather than public interests.⁵⁰⁹

A co-regulatory model is neither a full comprehensive law nor purely an industry self-regulation; rather, this is a combination of the two. In the co-regulatory approach, the government and industry share the responsibility of establishing and enforcing the standards.⁵¹⁰ The government's participation is to ensure that the developed standards provide a sufficient level of protection for people's private information and to ensure that the rules are enforced. The co-regulatory approach delivers the flexibility of self-regulation in addition to the supervision and rigidity of the government rules.⁵¹¹ Co-regulation has its drawbacks, however. Compared to the comprehensive law approach, this approach lacks transparency and accountability.⁵¹² Giving the industry the opportunity to negotiate the rules with the government and share the responsibility of enforcing these rules will often result in deals that work better for the industry rather than for the public interest.⁵¹³

Given the risks and the costs of adopting GDPR in developing countries, Tiffany Curtiss suggests that a co-regulatory model can be a wise choice for developing countries.⁵¹⁴ For Saudi Arabia, this might be a reasonable step to start with while working on building the foundation for a comprehensive law. The main difference between self-regulatory and co-regulatory approaches has to do with who establishes and imposes the goals and standards.⁵¹⁵ In a self-regulatory

⁵⁰⁹ *Id.*

⁵¹⁰ *Id.*

⁵¹¹ *Id.*

⁵¹³ *Id.* at 142.

⁵¹⁴ Curtiss, *supra* note 487 at 118.

⁵¹⁵ Dennis D. Hirsch, *The Law, and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 465 (2011).

model, the industry itself sets the goals, develops standards, and enforces these standards.⁵¹⁶ In a co-regulatory model, however, government and industry share the responsibility of establishing the standards and enforcing them.⁵¹⁷ There is no one particular form of this collaborative regulation. The government and private parties might split the tasks. For instance, the government might set the overall objectives, and the industry establishes and enforces the standards.⁵¹⁸ Another way to form the collaborative regulation is to have both the government and private sector work together to perform the same tasks.⁵¹⁹

In Saudi Arabia, co-regulation could provide meaningful privacy protection with reasonable costs to the public and private sectors, and more flexible standards. One of the issues in Saudi Arabia relates to a lack of technical skills and privacy policies within the government. In a co-regulatory mode, those with knowledge pertinent to the regulated area would establish the standards, as government organizations might not have technical skills or knowledge relevant to the regulated area.⁵²⁰ This would reduce government costs and produce effective and applicable rules that can work to address extant issues. Moreover, setting the standards based on the industry will help the government to establish suitable regulations for each sector depending on the sensitivity of the information and the ability of the industry to comply with the rule. For example, requiring each of the telecommunications companies to assign privacy officers might be reasonable because there are only three large companies and they have very sensitive data. On the other hand, it may be difficult to require every company that holds personal information,

⁵¹⁶ FINAL REPORT STUDY ON CO-REGULATION MEASURES IN THE MEDIA SECTOR, HANS BREDOW INSTITUT 17 (2006), available at <https://www.hans-bredow-institut.de/uploads/media/default/cms/media/cd368d1fee0e0cee4d50061f335e562918461245.pdf>.

⁵¹⁷ *Id.*

⁵¹⁸ *Id.*

⁵¹⁹ *Id.*

⁵²⁰ Curtiss, *supra* note 487 at 118.

including personal employee information, to appoint privacy officers. It is necessary, however, that a government official is involved in the regulation process, as this is essential in encouraging business to prioritize public goals over their own interests.⁵²¹

In Saudi Arabia, the National Cybersecurity Authority (NCA) may be the government body best suited to set overall goals for the private sector. NCA has technical experts who can best negotiate the standards with each industry. It is essential to define “personal information” and the overall goals before requiring each sector to come up with the best standards and rules by which to protect personal information. This step, which would raise awareness regarding and illustrate the importance of privacy professionals, will help the government to achieve its ultimate goal of building strong foundations upon which a comprehensive data protection law can be fully established and implemented.

Examining the current level of information privacy protection provided via Sharia principles as well as several regulatory measures, and exploring the obstacles that have led to this insufficient level of protection, permit the author of this dissertation to provide recommendations that will help to increase the level of protection. The recommendations include judicial, administrative, and educational reforms to create a solid foundation for new data protection laws. The proposals do not discuss a proposed data law in detail. While it is important to examine the law itself, and future research should consider this, this dissertation instead focuses on preparing a solid foundation upon which a comprehensive data protection law can be established.

3- Establishing an oversight authority

Establishing an independent data protection supervising commission is essential for both the short- and long-run. The commission could lead the transition period to a comprehensive data

⁵²¹ Hirsch, *supra* note 515 at 467.

protection law by negotiating with each industry regarding the best data protection standards, ensuring that companies comply with the established standards, reviewing the current regulations, providing guidance as it pertains to the interpretation of these laws, advising governmental institutions on how to protect people's personal information, and proposing new legislation. The commission should be free from outside influence, including governmental influence, and can thus enforce the law in both the public and private sectors. Commission members should have legal and technical backgrounds because privacy in the digital world requires a technical understanding of industry standard security practices.⁵²² The commission will continue to play a vital role if Saudi Arabia chooses to adopt a GDPR-like law in the future. Finally, publishing regular reports will help the public to become better educated regarding its privacy rights and serve to warn companies that violate the rules.

The commission might be under National Cybersecurity Authority (NCA), which was established by a royal decree. NCA is an independent public authority that is directly linked to the king.⁵²³ According to Alayban, the head of NCA, the authority "will begin its regulatory and operational role in cybersecurity by enhancing the protection of networks, IT systems, operating systems, hardware, software, services and data components, taking into account the growing vital importance of the Internet. Security in the life of the public."⁵²⁴ The objectives and independence of the NCA make it perhaps the most suitable body through which to establish a special data protection commission.

⁵²² Curtiss, *supra* note 487 at 118.

⁵²³ *King Orders Setting up of National Cyber Security Authority*, SAUDI GAZETTE, Nov. 1, 2017, available at <http://saudigazette.com.sa/article/520782/SAUDI-ARABIA/King-orders-setting-up-of-National-Cyber-Security-Authority>.

⁵²⁴ *Id.*

4- Judicial reforms

Many of the obstacles that have led to an insufficient level of privacy protection are the result of an ineffective juridical system. Most of the judges that are a part of the system are insufficiently qualified to apply general Sharia principles to today's privacy issues associate with the digital world. Further, the courts' decisions are inconstant regarding compensation for moral damages, which takes a considerable amount of the compensations awarded for privacy violations. Additionally, the judicial system does not recognize class-action cases, which are considered a useful tool by which citizens may sue companies for privacy violations. Reforming the judicial system is essential if individuals are to be granted meaningful access to remedies for privacy violations.

a. Establishing a judicial data protection committee

One way to solve the juridical obstacles is to form a special judicial committee for data protection. In Saudi Arabia, there are about 74 judicial and quasi-judicial committees that have jurisdiction over certain areas; these include the Committee for the Settlement of Banking Disputes, the Commercial Papers Committee, and the Committee of the Violations of the Telecommunications Law.⁵²⁵ These committees enjoy varying degrees of power regarding their decisions, and the committees' judges do not all hold the same qualifications.⁵²⁶ Establishing a special judicial committee for data protection will facilitate the other judicial reforms, allow for judges with specific skills to be chosen, and establish privacy norms.

One of the primary reasons to establish a special judicial committee is to create a body comprised of judges with strong backgrounds in specific areas.⁵²⁷ The privacy issues in today's

⁵²⁵ Youssef Alhdithi, *Aljihat Shbh Alqadaiya [Quasi-Judicial Bodies]*, CENTER OF JUDICIAL STUDIES SPECIALIST, 2009, at <http://www.cojss.com/article.php?a=226>.

⁵²⁶ *Id.*

⁵²⁷ *Id.*

digital world require technical knowledge, but in Saudi Arabia, it is also necessary for judges to hold certain qualification regarding Sharia law, as this permits a judge to practice ijihad. The existence of specialized judges will help to extend general Sharia principles so that they can be used to help decide today's issues. Moreover, the decisions of the committee should be published regularly so as to further build information privacy norms in Saudi Arabia.

b. Allowing class-action cases

As explained in the previous chapter, a class-action case is an essential tool to be employed when massive data breaches occur. The judicial system in Saudi Arabia does not allow class-action cases, however. Recently, the Saudi Capital Market Authority (CMA) issued a regulation that approves class-action lawsuits. The law aims to "protect investors and facilitate the procedures of litigation for the participants in the capital market, especially in cases where the plaintiff is a large group of persons, who share the same legal bases, merits and the subject matter of the requests, which is appropriate to the nature of the listed companies and the size of their shareholders."⁵²⁸ Class-action suits are only allowed before the Committee for the Resolution of Securities Disputes (CRSD). The same experience might be applied for privacy violations claims, since the plaintiff could also be "a large group of persons, who share the same legal bases, merits and the subject matter of the requests."

c. Compensating moral harm

Since many data protection violations may result in moral damages, such as distress, rather than immediate material damages, and the Saudi courts' decisions remain inconsistent regarding the compensation for moral harm, many individuals whose privacy rights are being

⁵²⁸ Capital Market Authority, *Chairman of Capital Market Authority: The regulations aim at protecting investors and facilitating the procedures of litigation for the capital market participants*, Nov. 22, 2017, available at <https://cma.org.sa/en/MediaCenter/PR/Pages/Class-Action-Suit.aspx>.

violated will face the risk of not receiving any compensations for such violations. Under GDPR, this may raise an issue of not providing data subjects with meaningful access to a remedy for privacy violations, and, therefore, Saudi Arabia will not be approved as a third-party country with an adequate level of data protection.

It is vital to recognize that the concept of compensating a morally harmed person exists in Sharia law as well as in some Saudi courts such as the administrative courts at the Board of Grievances. The issue at hand is that not all of the courts that have jurisdiction over information privacy issues award compensation to the morally harmed person. Thus, having a special committee for information privacy violations might effectively address this issue once the committee decides to compensate for moral harm.

5- Raising the level of privacy education

Education plays a critical role in building a solid foundation for a comprehensive data protection law. Both government institutions and private sectors will need both people and technical work to comply with the law. Saudi Arabia suffers from a shortage of technologists and privacy professionals. The Saudi government and educational bodies have already begun working on preparing technologists specialized in information security and cybersecurity in general, but there remains a need for privacy professionals.

Privacy courses and training programs in both the law and informatics schools or through for-profit or non-profit organizations can facilitate the training of privacy professionals. The government owns most of the educational institutions in Saudi Arabia, and this may serve to accelerate the process of establishing privacy courses and training programs once the government is eager to take this step. The private educational institutions, however, may be reluctant to follow suit until they believe that the market is in need of privacy professionals, which is not the case at present, given the country's lack of data protection regulations. Thus, the

government should assume the initiative to prepare privacy professionals. An even faster way to do this is to send students to study abroad in foreign countries that have more experience with privacy regulations. The National Cybersecurity Authority and the Ministry of Education have already taken this step as a means of training 1,000 students in cybersecurity and artificial intelligence over the next five years. Finally, the National Cybersecurity Authority and the Ministry of Education should work together regarding the preparation of privacy professionals who will be able to respond to market need when the pertinent law is applied.

To summarize the recommendations, adopting a comprehensive GDPR-like data protection law could serve as the best means by which to grant people a high level of privacy protection in the digital age. However, moving toward the adoption of a comprehensive law without first establishing a solid foundation, which would require, for example, an efficient judicial system, skillful technologists, and privacy professionals, might result in problems and could backfire on the Saudi technology market by increasing the risks and costs for both local and foreign investors. Thus, this dissertation recommends that Saudi Arabia consider pursuing an intermediate step, which would involve application of the co-regulatory model, while strengthening foundation upon which a comprehensive law can be built. The technology market plays a critical role in Saudi Arabia's future, so it is essential to prepare the market before enforcing a strict, comprehensive law.

The flexibility of the co-regulatory approach would allow the government to improve the level of data protection across different industries in a way that works best for each sector. Meanwhile, to reach its ultimate goal (i.e., a comprehensive data protection law), the Saudi government should work on reforming the judicial system so as to provide individuals with meaningful access to remedies when privacy violations occur. The government should also

prepare technologists and privacy professionals to serve the needs of both the government and private companies.

❖ Conclusion

The legal system in Saudi Arabia relies on both Islamic jurisprudence and written laws. This dissertation examines the efficiency and sufficiency of the legal protections granted to individuals regarding their personal information in accordance with both Sharia principles and current Saudi regulations. This dissertation also notes the primary obstacles that have served to reduce the level of protection afforded to individuals, and it has offered recommendations aimed at improving information privacy protection.

Islamic jurisprudence has developed several general principles that aim to protect individuals' privacy. These include the following: 1) prohibiting any intrusion, regardless of how the information is obtained, into individuals' homes, papers, or confidential conversations; 2) establishing a new set of rules that regulate how to seek permission before entering someone's house or coming between two people who appear to be having a private conversation in a public area; 3) maintaining the confidentiality of the individual's private information by criminalizing any disclosure of any information that may lead to another person's harm; 4) the order to conceal others' private information, especially confidential information that appears through a certain necessity such as a physician-patient relationship or a husband-wife relationship. These principles were developed prior to technology and, therefore, were able to provide a high level of protection regarding individuals' privacy at that time. The generality and the reliance on the general custom permitted these principles to be applicable in a number of different contexts.

Today, after the technological revolution, the amount of personal information available has increased considerably, and accessing such information has become much easier, which poses a higher threat to individual privacy. The Sharia principles and rules that protect information privacy need to be further developed so that they may provide individuals with the

same level of privacy protection as the principles intended to allow for and did allow for prior to the digital era. In theory, the Sharia principles should be applicable to modern privacy issues. However, applying these principles and rules to new issues requires judges with specific qualifications to practice *ijtihad*, which presents an obstacle due to the fact that most judges in Saudi Arabia are not classified as *mujtahid*. What makes the situation even more complex is that the courts' decisions are not regularly collected and made available to the public, and there are no precedents that are binding to other courts according to the Saudi Arabia legal system. Thus, the judges are not able to build on other judges' decisions. Additionally, the scarcity of Islamic jurisprudential research with regard to the protection of privacy in the digital age makes it increasingly difficult for judges to take on the task of deciding new privacy violations cases.

Additionally, there is no comprehensive data protection law in Saudi Arabia. However, many legal provisions relating to the sanctity and safety of individuals' personal data are spread out over several legislative instruments. Most of these regulations do not place information privacy among their primary goals. Instead, the regulations tend to utilize broad language when attempting to regulate matters related to information privacy. For instance, the Anti-Cybercrime Law incriminates any "invasion of privacy through the misuse of a camera-equipped mobile phone and the like" and any "production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through an information network or computer" without clarifying what constitutes an invasion of privacy.

Similarly, article 9 of the Banking Consumer Protection Principles, which is entitled "Data Protection and Confidentiality," holds the banks accountable for protecting and maintaining the confidentiality of consumer data, even if a third party holds the data, and providing a safe and confidential environment to ensure the privacy of consumer data. SAMA

imposes some detailed rules via seven administrative circulars, only two of which are available to the public. Further, the Law of Practicing Healthcare Professions (LPHP) has established broad rules aimed at protecting individuals' health information. Article 21 of the law requires that a healthcare professional shall maintain the confidentiality of information obtained in the course of his or her practice and may not disclose it without written consent from the concerned party except if the disclosure was to report a case of death resulting from a criminal act, to prevent the commission of a crime, or to report epidemic diseases.

In recent years, lawmakers have begun to pay more attention to information privacy, as demonstrated by their adoption of more detailed provisions that protect individuals' personal information. The Executive Regulation of The Telecommunication Law of 2018 specifically limits service providers' abilities to collect, disclose, and use consumers' information without their prior consent or legally grounded authority. Moreover, the Cloud Computing Regulatory Framework, issued by the Communications and Information Technology Commission in 2018, limits cloud service providers' abilities to transfer customers' content unless they notify their customers and, in some cases, obtain customers' explicit permission. Additionally, in case of a data breach, cloud service providers have to notify their customers of the breach incident or/and report to the CITC. Similarly, the draft of the E-commerce Law limits companies' abilities to retain customers' personal data longer than the transaction actually requires and prohibits companies from sharing consumers' personal and banking information with third parties unless they obtain written permission from the consumers.

Saudi Arabia's lack of a comprehensive data protection law results in multiple courts and judicial committees that have jurisdiction over information privacy issues. The multiplicity of courts that are entitled to hear cases concerning the protection of individuals' personal data has

made it more difficult to predict a court's decision since each of one these courts might be guided via different principles. A notable example of this involves the difference between the General Sharia Courts and the Board of Grievances regarding compensation for moral damage, which is a critical issue pertinent to receiving compensation for privacy violations. An additional obstacle has to do with the fact that none of these courts recognize class action cases, which play a very vital role in data breach cases.

Saudi citizens value their rights to privacy, but they tend to be unaware of how their privacy may be violated, including how the presence of technology can result in privacy violations. The number of data breach and privacy violation incidents, combined with the lack of any legal action, is indicative of this. Ambiguous regulations and weak education, especially education pertinent to information privacy laws, are the primary reasons why Saudi citizens have a low level of awareness regarding their privacy rights. Unlike the computing and informatics science schools, law schools in Saudi Arabia have yet to recognize the importance of teaching information privacy laws.

Adopting a comprehensive GDPR-like data protection law could serve as the best means by which Saudi Arabia can protect people's right to privacy as one of the human rights promised by both the Sharia and the Basic Law of Saudi Arabia and make the Saudi market a desirable market for foreign companies. However, the technology market plays a critical role in Saudi Arabia's future, so it is important to carefully prepare the market before enforcing a strict, comprehensive law. Adopting a comprehensive data protection law before first developing a solid foundation, which would require, for example, an efficient judicial system, skillful technologists, and privacy professionals could have a negative impact on the Saudi technology market by increasing the risks and costs for both local and foreign investors. On the other hand, building a strong foundation takes a long time, which means that it could be quite a while before the

country is ready to adopt such a law. Thus, this dissertation recommended that Saudi Arabia should consider pursuing an intermediate step, which would involve application of the co-regulatory model, while working on reforming the judicial system and preparing technologists and privacy professionals to strengthening foundation upon which a comprehensive law can be built. The flexibility of the co-regulatory model would permit Saudi Arabia to improve the level of data protection across different industries in a way that works best for each sector and reduce the cost and the risk on both the government and private sector.