Developing a Libyan information privacy framework

Mahmoud Mohamed EL-Sheikh
LLB University of Tripoli (Libya)
LLM (Coursework) QUT

A Thesis submitted in partial fulfilment of the requirements for the degree of Master of Laws (Research)

Faculty of Law
Queensland University of Technology
2013
Abstract

This thesis considers how an information privacy system can and should develop in Libya. Currently, no information privacy system exists in Libya to protect individuals when their data is processed. This research is designed to provide some illustration of the way forward for Libya and proceeds in four ways. First, it examines the importance of the right to privacy with respect to Sharia law and international treaties. Second, it reviews the two main approaches to regulating privacy, industry self-regulation and substantive legislative approaches, and concludes that a substantive legislative approach is more suitable for the Libyan context. Third, this thesis canvasses some of the most important features of information privacy law in order to identify the basic principles that a Libyan privacy law must consider, including issues of scope, exceptions, and core information protection principles. Finally, this thesis turns to the question of enforcement, including remedies and penalties and the establishment of a legitimate data protection authority. This thesis concludes that Libya should adopt a strong information privacy law framework and highlights some of the considerations that will be relevant for the Libyan legislature in doing so.
Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

QUT Verified Signature

Signature:

Date:  __20/12/2013________
Acknowledgements

My sincere gratitude to my principle supervisor Dr Nicolas Suzor for his incredible support during my study and to my associate supervisor Professor Reece Walters.

A very big thank you is said to my parents for their support and encouragement. The same is said to all of my family and my friends.

My special thanks to Beryl Besse who assisted me in finalising my work by providing editorial assistance.

Finally, I would like to thank my sponsor (the Libyan government) which makes this journey possible.
# Table of content

ABSTRACT .................................................................................................................. III

STATEMENT OF ORIGINAL AUTHORSHIP ................................................................ IV

ACKNOWLEDGEMENTS ............................................................................................ V

CHAPTER I INTRODUCTION ..................................................................................... 1

1.1 STRUCTURE .......................................................................................................... 1
1.2 METHODOLOGY .................................................................................................. 8
1.3 STRUCTURE OF THESIS .................................................................................... 9

CHAPTER II THE RIGHT TO PRIVACY ..................................................................... 13

2.1 THE DEFINITION OF PRIVACY ........................................................................ 13
  2.1.1 Privacy in the context of e-commerce ............................................................ 16
2.2 THE PROTECTION OF PRIVACY IN SHARIA LAW ........................................ 18
  2.2.1 Privacy of homes and correspondences ....................................................... 19
  2.2.2 Privacy and Islamic law of evidence .............................................................. 21
  2.2.3 Restriction on government ........................................................................... 22
  2.2.4 Privacy and the Islamic Declaration of Human Rights ............................... 23
2.3 PRIVACY IS A HUMAN RIGHT AND MUST BE SUITABLY PROTECTED .......... 25
2.4 THE IMPORTANCE OF E-COMMERCE IN DEVELOPING COUNTRIES ........ 27
  2.4.1 E-commerce in Libya ................................................................................... 30
2.5 CONCLUSION ...................................................................................................... 33

CHAPTER III THE MODEL OF PRIVACY PROTECTION – SELF-REGULATION OR LEGISLATIVE APPROACH ........................................................................ 35

3.1 SELF-REGULATION IS INAPPROPRIATE CHOICE FOR LIBYA ......................... 37
  3.1.1 Self-regulatory approach has theoretical flaws which limit its effectiveness ... 38
  3.1.2 The experience of the US suggests that self-regulation has not been highly effective ...
    A- Facebook and the US Federal Trade Commission (FTC) .................................. 45
    B- Google and the EU ........................................................................................... 46
    C- Evaluation ........................................................................................................ 47
  3.1.3 The conditions for successful self-regulation are not likely to exist in developing countries ...
    1 Self-regulation requires special conditions which are absent in developing countries ...
      (i) Consumers’ behaviour in developing countries .............................................. 53
    2 The practice of the self-regulatory model in developing countries ................. 55
      A - Voluntary Environmental Regulation .......................................................... 55
      (ii)- The Costa Rican practice ........................................................................... 57
      B- Self-regulation of Non-Government Organizations (NGOs) in developing countries .... 58
      (i)- Kenyan NGOs’ practice .............................................................................. 58
      (ii)- Botswana NGOs' practice .......................................................................... 59
    3. Conclusion for Libya ......................................................................................... 60
3.2 LEGISLATIVE APPROACH IS THE SUITABLE MODEL FOR LIBYA .................. 61
  3.2.1 Law provides adequate protection to individuals .......................................... 61
5.1.3.1 The requirements for establishing an effective Data Protection Commission ......................... 144
   A. Independence .................................................................................................................. 144
   B. Transparency ................................................................................................................ 149

5.1.3.2 The Malaysian and Moroccan experience ...................................................................... 151
   A. The Malaysian Data Protection Commission ................................................................. 151
   B. The Moroccan Data Protection Commission ................................................................ 154

5.1.3.3 The creation of the Libyan Data Protection Commission ............................................. 155
   1. Summary of the common requirements for establishing DPAs from other jurisdictions .... 155
   2. The Supreme Commission of Applying the Required Standards for Holding Public Positions .... 156
   3. The benefits of following the precedent of the Supreme Commission in establishing a Libyan Data Protection Commission .............................................................................. 158

5.2 REMEDIES AND SANCTIONS FOR CONTRAVENING DATA PROTECTION LAW ............... 161

5.2.1 Remedies ....................................................................................................................... 161
   5.2.1.1 Data Protection Commission orders ....................................................................... 161
   5.2.1.2 The court orders to redress privacy breach ............................................................ 164
   5.2.1.3 Compensation ......................................................................................................... 165

5.2.2 Sanctions ....................................................................................................................... 167
   5.2.2.1 Civil monetary penalty .......................................................................................... 167
   5.2.2.2 Criminal penalties .................................................................................................. 169
      1. Imposing Fines .............................................................................................................. 169
      2. Imprisonment ............................................................................................................... 170

5.3 CONCLUSION ...................................................................................................................... 175

CHAPTER VI CONCLUSION ..................................................................................................... 177
BIBLIOGRAPHY ....................................................................................................................... 185
Chapter I

Introduction

1.1 Structure

This thesis considers how an information privacy system can and should develop in Libya. Currently, no information privacy system exists in Libya to protect individuals when their data is processed. This research is designed to provide some illustration of the way forward for Libya and proceeds in four ways. First, it examines the importance of the right to privacy with respect to Sharia law and international treaties. Second, it reviews the two main approaches to regulating privacy, industry self-regulation and substantive legislative approaches, and concludes that a substantive legislative approach is more suitable for the Libyan context. Third, this thesis canvasses some of the most important features of information privacy law in order to identify the basic principles that a Libyan privacy law must consider, including issues of scope, exceptions, and core information protection principles. Finally, this thesis turns to the question of enforcement, including remedies and penalties and the establishment of a legitimate data protection authority. This thesis concludes that Libya should adopt a strong information privacy law framework and highlights some of the considerations that will be relevant for the Libyan legislature in doing so.

The Libyan Constitutional Declaration (2011) emphasises the right to privacy for everyone. The Constitution stipulates that

Correspondence, telephone calls and other means of communication shall have their own sanctity and their secrecy shall be guaranteed. They may not be confiscated or monitored except by a causal judicial warrant and for a definite period in accordance with the provisions of the law.¹

With regard to privacy protection, there are some provisions in the Libyan Penal Code (1953) that provide general protection for private correspondence and homes from any interference by others. These articles provide that the public servants who

¹ The Libyan Constitutional Declaration (2011), art (13).
commit an offence against private correspondence will face imprisonment of no less than six months.\textsuperscript{2} Also, there are some articles in the \textit{Act No 4 (1990) on the National System for Information and Documentation}, which governs the government’s collection of personal data for conducting research for social and economical reasons. This Act provides some provisions which require government entities to take some steps to protect the collected data, such as prohibiting the government from forcing individuals to give their data in order to conduct its research.\textsuperscript{3} However, these articles do not provide protection to personal data when individuals process their data.

Sharia law requires respect for an individual’s private life and this thesis provides examples of many circumstances where Sharia law indicates the significance of individuals’ privacy, whether in their homes or their correspondence. Because any Libyan legislation must comply with Sharia law principles, it is important to consider the position of Sharia law on the protection of privacy. Sharia law recognises the right to privacy and provides strong protection for a person’s private life which means the Libyan policy-makers can consider the right to privacy according to the international directions as long as those directions provide a strong protection to individuals’ privacy and there are no contradictions of Sharia principles.

This thesis adopts the position that privacy is a human right that should be strongly protected. However, privacy law must balance individual rights with economic interests. Nowadays, personal data has clear economic value for business. For example, the use of personal information in marketing can create new business opportunities and enable consumers to make better informed decisions. Greater access to consumer preferences may also enable businesses to better ensure that customer needs are met.\textsuperscript{4} The exchange of personal data is the foundation of services provided from businesses to consumers. Basically, many services offered by industry require firms to access personal data of clients, including, for example, debit and

\begin{thebibliography}{99}
\bibitem{2} The Libyan Penal Code (1953) ss 436, 244.
\bibitem{3} Act No 4 (1990) on the National System for Information and Documentation (Libya) ss 6, 7, 8.
\end{thebibliography}
credit card information. Therefore, the rise in the exchange of personal data which is linked with online businesses might lead to some positive outcomes which could provide greater opportunities for growing businesses.

The employment of technology and consumers’ data in business has encouraged innovation and as a result, such improvement has led industry to decrease expenses and meet consumers’ expectations. The former chairman of the Federal Trade Commission (FTC) in the USA claims, with regard to the value of new technologies in gathering personal information, that

(the) new medium (Internet) is also very valuable to merchants because it is used to collect vast amounts of personal information about consumers. Commercial sites on the World Wide Web (the "Web") collect personal information explicitly through a variety of means, including registration pages, user surveys, online contests, application forms, and order forms. Web sites also collect personal information through means that are not obvious to consumers, such as using electronic means (e.g. cookies) to track which pages a consumer views and for how long.

New technology makes the collection of personal data easier and sometimes, this occurs without the knowledge of consumers. This highlights the need to establish a privacy system which achieves a balance between the right of individuals to have their information adequately protected and the interests of businesses to use personal data which contributes to industry growth.

The free flow of data without privacy regulation might be harmful to consumers. A threat to privacy could be because firms collect a huge amount of data which because of a lack of data security, this information could be stolen, possibly causing damage to individuals.

References:

6 Lenard and Rubin, above n 4, 1.
9 Lenard and Rubin, above n 4, 1.
10 Ibid.
It seems that there is obviously great value in sharing personal information for businesses, but sharing individuals’ data raises real concerns regarding the protection that such valued information should have. Fears have been growing over protection from unwanted surveillance and utilisation of individuals’ information which include data related to some sensitive area such as medical records and employment reports, resulting from the improvement of computer technology and the subsequent capability for information collection and storage space.\(^\text{11}\)

Personal information should be adequately protected. The discussion above, however, suggests that such protection should not prevent all sharing of personal data, but should include some procedures to protect persons from misusing their data. Therefore, there is a need to find a suitable approach that provides adequate protection to individuals regarding their personal information.

This thesis examines two approaches which exist as methods of protecting personal information. The first approach is the self-regulation approach which is applied by some countries, in particular the United States.\(^\text{12}\) Self-regulation involves each industry in a specific business field taking the responsibility of establishing its own rules and enforcing penalties, as an alternative to being managed by government entities.\(^\text{13}\)

The self-regulation approach is the approach that stands beside the free market and is less focused on the protection of the individual.\(^\text{14}\) The advocates of self-regulation argue that this system supports the free market model which encourages innovation

---


and increases consumer options. Also, they claim that under this system, businesses have the capability to recognise the best standards for a specific industry and therefore principles will be realistic and firms will be adaptable to their policy.

However, there are real concerns about giving businesses or organisations the opportunity to establish their own policy as they generally would protect their own interests. Protection of personal information is a vital aspect of human rights and that means firms or organisations should not be given the power to determine policy in relation to such a serious matter. If businesses are given the power to choose their privacy conduct, then such policy will be weak in practice, because there is no method to enforce such policy and also, firms usually do not enforce privacy principles which may prevent them, in some circumstances, from sharing personal data. This study argues that the self-regulation approach, whether in developing or developed countries, is not working effectively from the perspective that privacy is a human right and accordingly, this approach will not provide sufficient protection of personal data.

The other approach is the legislative approach which has been adopted by many countries that provide protection of personal data. A legislative approach means that the policy-makers in each state introduce privacy law which aims to provide strong protection of personal data. Under the legislative approach, the system looks at personal information as a right of an individual and does not really consider economic growth as an important factor because the priority is protecting individuals’ personal information. The legislative approach asserts that direct government legislation adds confidence to consumers and as a result, increases commerce.

---


17 See France, England, Germany, Denmark, Australia, Canada, Malaysia, and Morocco as examples.

18 Swire and Litan, above n 14.

19 Peng Hwa Ang, above n 15, 3.
This study argues that the legislative approach provides adequate protection to individuals and also explains that there is no apparent evidence to suggest that there are negative impacts on economic growth if a legislative option is preferred. Finally, it argues that this approach will help to meet the requirement of adequacy ordered by the EU Directive 95/46/EC.\textsuperscript{20} The adequacy condition requires each state that deals the transfer of personal data with the EU to provide sufficient protection of personal data. Adopting a strong privacy law will make it easier for Libya to meet the EU adequacy principle. This will generally be important in order to accommodate business dealings between Libya and EU countries.

Adopting the legislative approach will stronger protection of any areas of privacy concerns because the state has the capability to force firms to abide by regulations and implement the policies of the state.\textsuperscript{21} Legislation is applied to all firms or industries if they fall under the scope of the law. Hence, there is no opportunity for businesses to disregard the application of such legislation.\textsuperscript{22}

This thesis concludes that the legislative approach is the preferred choice in the Libyan context. The protection of personal information is considered a human right and this right has been identified by many international treaties. These international treaties recognise the right to privacy as one of the most significant rights linked to human beings.\textsuperscript{23} It means that personal information should be under real protection from any illegal behaviour.

This means that if Libya follows such a recommendation and enacts a privacy law, some of the matters related to the law should be examined. These concerns include


\textsuperscript{22} National Consumer Council (UK), Models of Self-regulation: An Overview of Models in Business and the Professions (November 2000) 18 <http://www.talkingcure.co.uk/articles/ncc_models_self_regulation.pdf> at 28-8-2013.

\textsuperscript{23} See Universal Declaration of Human Rights, GA Res 217A(III), UN GAOR, 3\textsuperscript{rd} session, 183 plen mtg, UN Doc A/810 (10 December 1948); International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 150 (entered into force 23 March 1976); Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, 213 UNTS 221(entered into force 3 September 1953).
the scope of the law, as it is important to recognise in which circumstances privacy law might not be applicable. Another concern is the issue of how to deal with personal information in areas such as processing and securing data. The last concern is linked to enforcement issues.

With regard to the scope of privacy law, this thesis argues that in order to have strong information privacy law, any legislation should be wide in its scope. Fewer exceptions on data protection law should be the direction of Libyan policy-makers as that will add more credibility to a privacy Act. Once privacy law stipulates many exemptions to its application, that might lead to a reduction in the integrity of the legislation.

Furthermore, this thesis examines the basic principles for dealing with personal data such as notice, choice and security principles. In particular, with regard to the right of consent, the study argues that the opt-in choice provides more adequate control to stakeholders than the opt-out choice and that the opt-in choice will be compliant with Sharia law. The value of examining these principles is that by adopting these principles, the most important areas of concern that arise for consumers will be considered.

Finally, the thesis focuses on enforcement issues; in particular, it aims to find a strong mechanism of enforcement. This issue is really important because without enforcement methods, any legislation will be weak and easy to breach. Commonly, privacy laws introduce privacy supervisory agencies which aim to monitor and control how traders or businesses deal with personal information. This study argues that it is vital to establish such a commission in order to supervise the processing of personal information. The study explains some of the most valuable functions that are commonly exercised by such supervisory agencies. It argues that such agencies play a vital role in enforcing privacy law in many circumstances such as enforcing penalties, providing explanations of unclear provisions and also contributing to the public’s awareness regarding protection of their privacy. The proposal of creating data protection commission is presented and the proposal follows the international requirements for establishing an effective supervisory agency in terms of independence and transparency.
In addition to creating a data protection commission, the thesis argues that data protection law should introduce remedies and sanctions which should be severe enough to deter potential offenders from infringing the law. The issue is that without strict sanctions such as imprisonment, the deterrence will be weak. These sanctions might be varied depending on the types of offences that are committed. Thus, fines and imprisonment should be the choice of any privacy law in order to punish any infringements of the law.

1.2 Methodology

This thesis adopts a doctrinal approach in order to identify the principle features of national and regional privacy regimes. Primary and secondary sources including national laws, international agreements, and academic commentary and the reports of law reform bodies were examined and critically evaluated. In order to obtain an understanding of the available policy choices in contemporary data protection law, this thesis undertook a broad survey of the statutory frameworks of several key jurisdictions. In particular, the United Kingdom and Australia were chosen as exemplars of developed common law countries with strong and well-established data protection regimes. These case studies were supplemented with analysis of the European Union’s data protection framework, which provides guidance for many civil law countries. Importantly, at such a high level of analysis, the differences between common law and civil law approaches were minimal, and common themes and distinct approaches were able to be identified across the range of legislative frameworks. This survey of established privacy law in developed countries was further supplemented by an examination of applicable legislation in Malaysia and Morocco, which share several key social, economic, and cultural characteristics with Libya; particularly, these countries are each developing nations with a strong Islamic culture.

Importantly, this thesis does not undertake a full comparative analysis of data protection law in these jurisdictions. Instead, the goal is to identify some common themes and diverging approaches which might illuminate the range of potential policy approaches for Libya. Similarly, as Libya is at an early stage of development with regards to privacy law, it was not possible to engage fully with emerging and
highly contested debates about the scope of contemporary data protection law. For example, new debates around privacy reform in the European Union and other jurisdictions were not able to be addressed within the scope of this thesis. Instead, this thesis provides a high level analysis of the features of existing privacy regimes in order to suggest some recommendations to the Libyan policy-makers. Necessarily, this thesis outlines only the foundations for a Libyan data protection framework; more detailed study on the specific features of a Libyan law must be left for future work.

In order to evaluate the doctrinal choices available, this thesis adopts a theoretical framework that views privacy as a fundamental human right and prioritises the requirements of Sharia law in implementation of domestic privacy principles.

1.3 Structure of Thesis

Chapter two is designed to discuss the meaning and importance of protecting information privacy. It reviews some definitions of privacy and considers the importance of privacy to e-commerce. In addition, the right to privacy under Sharia law is examined and some evidence which supports the protection of a personal life according to Sharia law is provided. Several international treaties which consider the right to privacy to be a fundamental human right are presented in this chapter. The final part of the chapter illustrates the value of e-commerce in developing countries and particularly in Libya, as the state considers the potentially strong markets of electronic commerce in the future.

In chapter three, two approaches to privacy protection are presented and evaluated, according to the practices of countries which have adopted those approaches. This chapter explains that self-regulatory approach has theoretical flaws which limit its effectiveness. The chapter also examines the application of the self-regulation model in the USA and illustrates how, from a perspective that privacy is a human right, the self-regulation approach has not been sufficiently effective in protecting consumers. With regard to developing countries, the study demonstrates how developing countries lack the requirements necessary to implement the self-regulation approach effectively. Examples indicate such limitations are presented particularly in the area
of voluntary environmental regulations and self-regulation of non-government organizations (NGOs).

The final part of chapter three argues that a substantive legislative approach is more suited to the Libyan context. A substantive legislative model provides more adequate protection of personal information and also this approach does not show negative impacts on business growth. Finally, adopting this approach will assist in developing a commercial relationship with the EU countries by more effectively meeting the adequacy requirement.

Chapter four of this thesis examines the enactment of a privacy law. Firstly, the chapter studies the scope of data protection law and in particular, considers some of the most important terms that are usually presented in data protection law and then examines some exceptions which might be adopted in any future Libyan privacy law. Secondly, privacy principles which are commonly adopted in the majority of worldwide data protection laws are studied and evaluated. These principles consider how businesses or organizations are required to deal with personal data in terms of processing such information.

Chapter five considers the importance of ensuring that there are adequate and appropriate methods of enforcement of data protection law. This chapter firstly examines the importance of creating a legitimate Data Protection Authority responsible for providing oversight of information privacy law. This chapter then reviews the requirements that such an authority must meet in order to work effectively, in particular independence and transparency. This thesis provides a proposal for the establishment of an independent Libyan data protection commission that can help Libyan policy-makers establish a strong supervisory agency. The second part of the chapter reviews remedies and penalties of various privacy regimes and highlights issues relevant to enforcement in Libya.

The final chapter of this thesis summarises some of the arguments that have been provided in previous chapters and then makes some recommendations that aim to help the Libyan policy-makers develop and establish a strong system of protection of personal information. In particular, these recommendations reflect the need to
enhance public awareness regarding privacy matters and also the need to establish a strong mechanism for the effective enforcement of the law.
Chapter II

The right to privacy

This chapter will discuss the meaning of privacy in general and also with regard to the context of e-commerce. In doing so, the definitions of privacy that were provided by different commentators are discussed in order to get a clear indication regarding the meaning of the right to privacy. This study is focusing on Libya and therefore, the right to privacy according to Sharia Law is examined as Sharia law is the basis of legislation in Libya and each law in Libya must comply with it. Examples which provide illustrations about how Sharia Law protects the right to privacy in different circumstances are used. Several international conventions which consider the right to privacy to be a fundamental human right are presented. Finally, the importance of e-commerce in developing countries is examined by presenting the positive effects of shopping online for the growth of the economy in developing countries and specifically for the Libyan economy.

2.1 The definition of privacy

It is vital to the study to present definitions of the term ‘privacy’ in general concepts. Furthermore, the concept of privacy in the area of e-commerce is discussed and presented as it is important to understand the notion of privacy with regard to the online business environment.

The concept of privacy has been under debate and discussion by many commentators worldwide. Some problems with the definition of privacy are attributed to the idea that privacy is a complex notion because ‘rituals of association and disassociation are

24 Article 1 of the Libyan Constitutional Declaration (2011) stipulates that ‘Islam is the Religion of the State and the principal source of legislation is Islamic Jurisprudence (Sharia)’.

25 Warren and Brandeis, in their article ‘The Right to Privacy’, stated that the law has been developed steadily. They said that the right to life was developed to include ‘the right to enjoy life [and] the right to be let alone’. Samuel D Warren and Louis D Brandeis, ‘The Right to Privacy’ (1890) 4 (5) Harvard Law Review 193.
cultural and species-relative’. An example of this is entering a house without knocking a door. This action can be understood in different ways because it might be regarded as a real privacy contravention in one culture but accepted in another.

Some commentators see privacy as a derivative concept that is linked to other fundamental rights and thus, it is not a separate right. This consequentialist definition of privacy is problematic given that the right of privacy is inherently linked to individuals’ interests. This chapter argues that in light of Sharia law and international conventions, privacy is better considered to be a fundamental human right.

Alan Westin proposed the following definition of privacy: ‘privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’. According to Westin the right to privacy for the individual consists of ‘the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public’.

The simplest definition may have to include a list of the individual’s authority over his or her information. For example, privacy can be considered to be the power of any person to practice his or her life with the least amount of interruption. According to this notion, persons ought to be protected against

- interference with family life and home living;
- interference with ethical rights and intellectual freedom;
- assaulting reputation and honour;
- disclosure of unrelated, embarrassing details;
- utilising a name, personal identity or picture;

27 Ibid.
28 Ibid.
30 Ibid.
f. spying or snooping on personal life;
g. viewing communications or misusing private correspondence (written or verbal);
h. divulging information given or received in confidence.\textsuperscript{32}

W A Parent has defined privacy by stating that ‘privacy is the condition of not having undocumented personal knowledge about one possessed by others’.\textsuperscript{33}

Personal information consists of facts which most persons in a given society choose not to reveal about themselves (except to close friends, family, . . .) or of facts about which a particular individual is acutely sensitive and which he therefore does not choose to reveal about himself, even though most people don’t care if these same facts are widely known about themselves.\textsuperscript{34}

Ruth Gavison, with regard to the definition of privacy, claims that privacy is a limitation of others’ access to an individual. As a methodological starting point, I suggest that an individual enjoys perfect privacy when he is completely inaccessible to others. This may be broken into three independent components: in perfect privacy no one has any information about X, no one pays any attention to X, and no one has physical access to X.\textsuperscript{35}

Daniel Solove, in his book ‘Nothing to Hide’, said that privacy can be attacked by the revelation of someone’s secrets and also it might be invaded by spying on someone else, even if no secret data was revealed by such an action. The harm in the revelation of undisclosed information is that someone’s hidden data is distributed to others. The damage in spying behaviour is that even if no personal data was revealed, a person might find such behaviour scary.\textsuperscript{36}

It seems that the abovementioned definitions recognise privacy in different ways. Some suggest that privacy is not even a separate right and that privacy is linked to

\textsuperscript{32} Ibid.


\textsuperscript{34} Ibid 270.


other rights. However, others provide strict definitions to protect privacy by stating that no one should have any information about individuals.

For the purpose of this thesis, I focus on a definition of privacy that focuses on control over personal information in the online context. Privacy is that individuals have the power to control or organise data about themselves without any intrusion. This privacy right provides a power to a person: the right of using or controlling personal data. As a result of individuals’ control and access over their rights, persons will be afforded the freedom to develop themselves as they believe they should.37

2.1.1 Privacy in the context of e-commerce

In the era of online transactions, it is hard to transact without providing some personal data such as address or favourite products. However, consumers might be reluctant to offer this required information in a situation in which they believe their privacy is in danger.38

Customers who purchase online normally evaluate the risk that may occur when they use online transactions as their data may be misused or revealed without their acceptance. Growing concerns over trust and data protection in online trade may suppress e-commerce.39

Online trust is assumed to have a fundamental effect in an e-commerce environment. ‘[M]any millions of dollars of e-commerce can be conducted if customers’ concerns, including privacy, can be adequately addressed’.40 Wu et al explain:

Online privacy concern leads to a lack of willingness to provide personal information online, rejection of e-commerce, or even unwillingness to use the Internet. Consumer concerns over privacy not only limit the development of electronic commerce, but may also affect the validity and completeness of

37 Moore, above n 26, 414.
40 Ibid.
consumer databases, which may lead to inaccurate targeting, wasted effort, and frustrated customers.\textsuperscript{41}

Conversely, access to personal data can also bring efficiency gains for businesses. As a result of markets getting access to personal data, they will have a better chance to gain many benefits which include identifying the best scenario for getting consumers.\textsuperscript{42} Regarding customers benefits, as a result of business access to private data, businesses may be able to provide consumers with access to a large number of products and acquire products from their own locations.\textsuperscript{43}

Privacy rights should not mean that no one can have access to someone’s private life because there should be a balance between an individual’s privacy and the ability of others to access some data related to individuals. In areas like education, health and national security, real restrictions should be enforced to defend such valued data. It is vital in some circumstances to get access to individuals’ data but this should only be with the knowledge of the owner of this data. In other areas, where sensitive information is not in issue, a less restrictive scheme may deliver a more appropriate balance.

In determining an appropriate balance between privacy rights and access to individual information, it is important to this study to examine the context of privacy in Sharia law which is considered by many constitutional declarations in Muslim countries, including Libya, as a main source of legislation.\textsuperscript{44} The next discussion shows evidence which demonstrates that Sharia law respects the concept of someone’s privacy.

\textsuperscript{41} Ibid.
\textsuperscript{43} Ibid.
\textsuperscript{44} See the Libyan Constitutional Declaration (2011) art 1.
2.2 The protection of privacy in Sharia Law

It is vital to examine the concept of privacy according to the principles of Sharia jurisprudence that is derived from the Quranic and the Sunnah (the teachings and practices of Prophet Muhammad) texts which are considered to be the main sources of law in Islam.

Sharia law recognises human rights that are essential for all individuals. Basic human rights which are adopted by constitutions and universal conventions are implemented by Sharia law. The value of existence, privacy, and liberty is an essential part of Sharia law. The Quran disallows any actions that cause scandals and defamation of other people, to protect their sanctity of life. This is apparent from this verse of the Quran:

O you who have believed, let not a people ridicule [another] people; perhaps they may be better than them; nor let women ridicule [other] women; perhaps they may be better than them. And do not insult one another and do not call each other by [offensive] nicknames. Wretched is the name of disobedience after [one's] faith. And whoever does not repent - then it is those who are the wrongdoers.

Sharia law totally accepts the protection of the privacy of someone’s house and personal life; and hence, respecting the individual’s right to privacy is one of the fundamentals of Islamic principles. Sharia principles provide many examples that indicate the right to privacy according to Sharia law. For example, people should be protected from spying by others and that prohibition of snooping is linked to individuals as well as Islamic governments because Islamic administrations are prohibited from looking at individuals’ secrets. The Prophet Muhammad (PBUH)

---

45 It should be note that Quranic and the Sunnah texts are considered to be the main source of law in Islam. Therefore, legal principles are based on or derived from these texts; and thus, Muslim jurists can derive principles from these texts as they can understand the context of these sources.

46 Muhammad Aslam Hayat, ‘Privacy and Islam: From the Quran to Data Protection in Pakistan’ (2007)16 (2) Information and Communications Technology Law 137.

47 Ibid.

48 The Noble Quran (Sahih International Trans) 49: 11.

49 Hayat, above n 46, 137.

states that ‘if you start prying into the secret affairs of the people, you will corrupt them, or at least drive them very near corruption’. This is clearly respectful of an individuals’ private life because it requires that others do not interfere into any person’s private life as the prophet said that that will negatively affect those persons.

Ida Madieha Azmi describes the theory of privacy rights according to Sharia law as divided into two ‘normative frameworks’: the first one is a ban on the interference in someone’s private life and the other is the orders and rules for maintaining secrets. ‘Included in the first category is the prohibition against espionage, trespass and eavesdropping. The second category includes keeping secrets of others in the context of a marital relationship, personal sins and information imparted to others in confidence’. According to this notion, a great number of Muslim scholars view personal privacy as a basic individual rights.

Sharia law texts ensure the protection for individuals’ privacy as a valued human right, and also many scholars indicate that the sanctity of individuals’ privacy is guaranteed in Islamic society. In the following discussion, some examples that explain the protection of privacy according to Sharia law will be provided. These examples are provided to show the importance of individuals’ privacy in Islamic society, from protecting privacy at home to defending privacy according to the Islamic law of evidence.

2.2.1 Privacy of homes and correspondences

Sharia law in both the Quran and Sunnah texts respects all individuals’ right to keep their own privacy under strong protection from interference from others, regarding the place where they live or the way they communicate. It is vital to this study to provide some evidence from the Quran and Sunnah texts to support such protection for persons in those specific circumstances. The prophet Muhammed said, regarding

---

51 Peace Be Upon Him.
52 Cited in Zulfiqar Ahmad, above n 50, 64.
54 Ibid.
55 Ibid.
the protection of property, that ‘verily your blood, your property are as sacred and
inviolable as the sacredness of this day of yours, in this month of yours, in this town
of yours’.

Allah says in the Quran:

O you who have believed, do not enter houses other than your own houses until
you ascertain welcome and greet their inhabitants. That is best for you; perhaps
you will be reminded. And if you do not find anyone therein, do not enter them
until permission has been given you. And if it is said to you, "Go back," then go
back; it is purer for you. And Allah is knowing of what you do.

Also, with regard to get permission before accessing private life, the Hadith (the term
‘Hadith’ refers to reports of statements or actions of the prophet Muhammad -
PBUH- or of his tacit approval or criticism of something said or done in his
presence) says that ‘Asking for permission is allowed up to three times. If it is not
granted, you must return’. The Quran evidently prohibits spying and negative
assumption as such activities cause offense to the individual’s right to privacy:

O you who have believed, avoid much [negative] assumption. Indeed, some
assumption is sin. And do not spy or backbite each other. Would one of you like
to eat the flesh of his brother when dead? You would detest it. And fear Allah;
indeed, Allah is accepting of repentance and Merciful.

It is apparent from the above text that the Quran recognises the value of everyone’s
right to privacy by suppressing spying on each other. The Quran describes someone
who spies on others as liking to eat the flesh of his dead brother. This description
provides evidence of how strongly Sharia law considers the significance of privacy.

‘The prohibition of spying also includes opening of personal letters and confidential
correspondence’. This principle is stipulated by the Hadith ‘one who looks into the
letter of his brother without his permission is like looking into the fire of Hell’.

---

56 Sahih Muslim, Book 7, The Book of Pilgrimage (Kitab Al-Hajj), ch 17, no 2803 a.
58 Sahih AL-Bukhari, Hadith 6317.
59 The Noble Quran (Sahih International Trans) 49:12.
60 Mohammad Hashim Kamali, 'Islamic Perspective on Personal Privacy' Saudi Gazette 3 May 2010
1 June 2013.
61 Cited in Ibid.
Moreover, the Prophet Muhammad states that ‘visitors must not stand in front of the houses’ doors when they seek permission to enter them’. The Prophet also (PBUH) said, ‘if one’s eye has entered a private place, the person her/himself has entered’.

According to the abovementioned sources from the noble Quran and the narration of Prophet Muhammad (PBUH), it is obvious that the sanctity of private life has been an important aspect of Islamic society and thus the protection of privacy is seen as a human right for every individual in the community.

From the Quranic and prophetic principles about the conditions for entering houses, the principle of prior consent can be derived from the condition of asking permission to entering homes. It is obvious that Sharia law, in order to protect the sanctity of private life of individuals, requires individuals to get clear permission from the resident of a house before the potential visitors can enter that house.

To the extent that electronic information can be likened to personal information in private places, this suggests that the principles of protecting privacy of homes and correspondences may be applied on electronic information. This suggests that a strong privacy regime is likely to be important under Sharia law.

### 2.2.2 Privacy and Islamic law of evidence

Another indication that privacy is deeply protected in Sharia is the principles of law of evidence. In order to protect privacy, the Sharia principles of evidence guarantee to every person the protection of his or her privacy in a variety of ways as can be seen in several texts and juristic analysis.

The Prophet Mohammed turned his face away (two times) from a man who sought to admit that he committed adultery. Only subsequent to the man’s insistence on making his admissions for the fourth time, did the Prophet examine the proposition that the person’s psychological condition may have induced him to make his

---

62 Al Hafid Al Hytami, Majmah Alzweed and Manbaa Alfawaed (Dar Alfikr Alarabi, Beirut, 1992) p 88, 12808.


64 Ibid.
confession. Basically, after the exclusion of these factors, the penalty was applied. This is clear evidence that Sharia law respects the sanctity of the private life of individuals. People are not forced to give any information about themselves when they breach the obligations of Sharia law in their private place and indeed, they are encouraged not to do so. People in their private place are independent and the single condition that is applied to this personal independence is that the individual behaviour must not damage anyone else.

Another example of the protection of privacy offered in the Islamic law of evidence is that Muslim scholars affirm whose unwillingness to permit the evidence of individuals when it is made for or against relatives. The reason for that is because family members are those mainly familiar with the details of every other’s private affairs. The suggestion is that even though scholars have not applied the term of ‘privacy’ to avoid such evidence, their approach has indeed been directed to the protection of an individual’s privacy.

It is evident from the abovementioned circumstances that the law of evidence according to Sharia law provided restrictive rules about accepting witness statements when there is a special relationship between individuals. Such a condition shows a good example of the protection of privacy in the Islamic community.

2.2.3 Restriction on government

During Islamic history, many indications from the practice of Islamic authorities provide evidence regarding the protection of individuals’ privacy in an Islamic state. These indications suggest that even the head of the Islamic state should not be allowed to get access to private life of persons. The following story illustrates such restriction.

Omar Bin Khattab, the second caliph, while he was travelling at night in a city, heard a noise and cursing which was coming from a residential area. He then tried to

65 Sahih Albokari, Hadith No 6439.
66 Hayat, above n 46,144.
67 Ahmad Atif, above n 63.
68 Ibid.
discover the reason for these loud voices that were coming through houses, so Bin Khattab tried to peek into the house and said to a man who was in that residence:\(^69\)

\[you, \text{the sinner, do you think that Allah will ignore your sins, as you’re sinning against him?}\] The man replied, if I sinned once, you sinned three times. Allah has forbidden you to look into someone’s fault, and you have done otherwise. Allah has commanded you to enter peoples’ homes through the front door, and you have intruded over the fence. And you have approached me without salutation, and Allah has commanded you not to enter into other peoples’ homes without their permission, and without saying ‘greetings’ (Salam) when you enter their premises.\(^70\)

The Caliph left the man’s house and asked him to repent of his sin.\(^71\)

Maududi, an Islamic scholar, states that the Islamic principle of \textit{Amr-bil-Maroom -wa-Nahi-anil Munkar}, to enjoin the good and to forbid the evil, does not permit the government to attack individual’s private life.\(^72\) Another clear example of restriction is the role of a \textit{Muhtasib}.\(^73\) The \textit{Muhtasib} ‘is not allowed to investigate or invade people’s privacy, even if they are committing sin in their privacy’.\(^74\)

Ghazali, an Islamic jurist, said that the \textit{Muhtasib} is not allowed to try to get information about a sin that is committed by an individual in his home behind closed doors. He also declares that ‘a person carries his privacy with him, and the \textit{Muhtasib} can judge only on prima facie appearance’.\(^75\) These restrictions on government collection of personal information imply that Sharia takes the issue of privacy seriously.

\textbf{2.2.4 Privacy and the Islamic Declaration of Human Rights}

\(^70\) Hayat, above n 46.140-141.
\(^71\) al-Ghazali, above n 69.
\(^72\) Zulfiqar Ahmad, above n 50, 57.
\(^73\) ‘The Muhtasib was certainly in charge of weights and measures, but he was also in charge of standards generally - even standards of public behaviour. He was, moreover, backed by a body of inspectors who were empowered to make regular checks on all the shops in the city, and to arrest offenders’. Caroline Stone, ‘The Muhtasib’ (1977) 28 (5) \textit{Saudi Armco World} 22.
\(^74\) Zulfiqar Ahmad, above n 50, 57.
The strong protection of privacy in Sharia can be seen clearly in the *Islamic Declaration of Human Rights*. The Nineteenth Islamic Conference of Foreign Ministers (Session of Peace, Interdependence and Development), held in Cairo, Arab Republic of Egypt 1990, introduced the *Cairo Declaration on Human Rights in Islam*. Article 18 of this Declaration stipulates that:

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

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

c. A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and its dwellers evicted.\(^{76}\)

Prior to the *Cairo Declaration*, the *Universal Islamic Declaration of Human Rights* stipulates that every person is entitled to the protection of his privacy.\(^{77}\)

It is evident that Islamic jurisprudence provides a real protection for the privacy of individuals in their homes, work places and communication. Thus, the general rule is that the protection of an individual’s privacy is guaranteed under the Sharia law unless there is inconsistency between the right of privacy and the scope of Sharia law.\(^{78}\)

To sum up, Maududi argues that no one has the right to spy on others, it is illegal according to by the Sharia law, ‘whether spying is done because of suspicion; for causing harm, or for satisfying one’s own curiosity’\(^{79}\)

The importance of privacy in Sharia law accords well with the treatment of privacy as a human right in the international context. Several international treaties consider the right to privacy to be a fundamental human right.


\(^{77}\) *Universal Islamic Declaration of Human Rights* (19 September 1981).


\(^{79}\) Maududi, cited in Zulfiquar Ahmad, above n 50, 64.
2.3 Privacy is a human right and must be suitably protected

Privacy is considered by many international treaties as a human right and accordingly, this right must be sufficiently protected. This section will examine how international agreements deal with the right to privacy.

Two theories have been adopted to determine the value of privacy. The first theory recognises protection of personal information as a basic human right. However, the second theory of privacy protection values the economy more than other factors and thus a market approach is chosen as a tool for privacy protection. It is suggested that privacy is

[a] fundamental human right that allows the individual the space that is necessary to develop her identity free from governmental control. Privacy, therefore, is a vital element of being human, one that is necessary to preserve democracy and a civil society.

‘Privacy is like freedom: we do not recognise its importance until it is taken away. In that sense, it is a personal right that we assume we have yet, take for granted - until something or someone infringes on it’. Therefore, the protection of privacy is the protection of one of the fundamental rights that should be valued and guaranteed for all citizens in any country. A number of international conventions has recognised the right to privacy and require clear protections for such a fundamental right. Some of these treaties are as follows:

A- United Nations’ Universal Declaration of Human Rights

Article 12

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

81 Ibid.
B- The International Covenant on Civil and Political Rights 84

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference.

C- American Convention on Human Rights 85

Article 11

Right to Privacy

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

2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation.

3. Everyone has the right to the protection of the law against such interference or attacks.

D- The European Convention for the Protection of Human Rights and Fundamental Freedoms 86

Article 8 87


87 The European Court of Human Rights delivered judgment in *Copland v. United Kingdom* [2007] ECHR 253 found that the UK had infringed the Copland’s right to respect for her personal life and correspondence under Article 8 of the European Convention on Human Rights. The fact in this case as follows:

‘In 1991 the applicant was employed by Carmarthenshire College (“the College”). In 1995 the applicant became the personal assistant to the College Principal (“CP”) and from the end of 1995 she was required to work closely with the newly appointed Deputy Principal (“DP”).’ At 7-8.

During her employment, the applicant's telephone, e-mail and internet usage were subjected to monitoring at the DP's instigation. According to the Government, this
Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

These international treaties consider the right to privacy as a fundamental human right and suggest that steps should be put in place to protect the right to privacy because everyone should have the right to freedom and to live without intrusion from others. Based on this strong respect for privacy in both Sharia law and international law, this thesis proceeds from the proposition that privacy is a human right that should be strongly protected.

2.4 The importance of e-commerce in developing countries

It is important to demonstrate the value of e-commerce to the economy, particularly in developing countries. A strong privacy system can provide a suitable environment in which to develop successful e-commerce practices. Therefore, this section provides the positive effect of e-commerce on business growth in developing
countries generally, and then particularly in Libya. However, while privacy must be strongly protected, it is not absolute. It must be balanced with the needs of development.

Since the emergence of the Internet, many aspects of our lives have been changed. The Internet has given us, for example, the opportunity to communicate, research and shop more easily. The positive effect of e-commerce can be seen more in developing countries as e-commerce plays a vital role in enhancing efficiencies and escalating productivity. With regard to such value Kofi Annan, the former UN Secretary-General, said that

\[\text{[e]-commerce is one of the most visible examples of the way in which information and communication technologies (ICT) can contribute to economic growth. It helps countries improve trade efficiency and facilitates the integration of developing countries into the global economy. It allows businesses and entrepreneurs to become more competitive. And it provides jobs, thereby creating wealth.}\]

E-commerce facilities allow access to a huge amount of data and more opportunities than traditional trade because this new technology allows for the spread of information across the world and contact with people in almost every State. The advanced facilities of e-commerce can assist corporations to gain more profits.

In addition, e-commerce is an activity that has assisted many countries to reach a higher level of development in recent years. E-commerce brings to manufacturers in developing countries the ability to enhance competition and customer services and

---


the opportunity to acquire access to the international marketplace at reasonable prices and for small amounts of investment.\textsuperscript{92}

E-commerce allows producers in developing countries to beat traditional restrictions that are caused by limited access to data, the high cost of market-entry, and exclusion from potential markets.\textsuperscript{93} Furthermore, firms in developing countries may have opportunities to broaden their global profile and to develop direct trading links with international customers and businesses. Additionally, it can accelerate the capacity of companies in developing countries to get information about consumer necessities in developed countries.\textsuperscript{94}

A study conducted by the London School of Economics regarding e-commerce in developing countries suggested the following policy implications of encouraging the B2B e-commerce model:

1. B2B e-commerce is essential for market access and export growth. Developing country governments must give priority to ensuring that the conditions for the participation of their businesses are met.

2. B2B e-commerce transactions are complex and information-intensive. The ICT infrastructure must be sophisticated enough to handle the data required. A quantum leap in telecommunications capabilities may be required.

3. Governments should ensure that telecommunication services are modern and efficient in order to lower the prices of network usage through effective competition and market liberalisation. Governments should also reduce tariffs to support trade in ICT hardware and software.

4. A legal framework to support electronic transactions has to be in place in order for firms to buy and sell on-line. This framework must include effective authentication and certification mechanisms (ie. Digital signatures, secure settlement procedures) and a means of protecting against on-line fraud as well as achieving redress in cases where disputes arise.

5. Significant amounts of business will migrate to B2B e-marketplaces with complex requirements. Governments should support investment in human resources.


\textsuperscript{93} Ibid.

\textsuperscript{94} Hamed, above n 90, 58.
6. Governments must ensure that national regimes for taxation, security and privacy protection are compatible with international governance regimes.\textsuperscript{95}

It is obvious that there many necessities in order to implement an effective e-commerce system in developing countries. The study indicates the value of meeting the above requirements as it is important to have competent ICTs in the country, human resources and a legal system encompassing many arenas. One of the policies which governments in developing countries should consider is the compatibility of privacy protection with international regimes in order to have a successful e-commerce system.

\textbf{2.4.1 E-commerce in Libya}

There is no doubt about the notion that electronic commerce will bring several benefits to developing countries, but African countries may have to overcome a number of issues before they can properly benefit from online trade.\textsuperscript{96} Such issues include the limited improvement of their economic systems which leads to slow economic growth and limited income per person. There are limited numbers of online users available to create an internet customer base, there is a lack of knowledge about the processes of e-commerce, such as credit card usage, and lastly, there is a limited number of people with the necessary skills to establish e-commerce services. In addition, a vital obstruction may be linked to the incredibly inadequate information and communication infrastructure that presently exists in the majority of African countries.\textsuperscript{97} Adopting modern rules and regulations that are essential to enhance the exercise of e-commerce might be quickly done, but improving the ICT infrastructure which is necessary to gain the complete advantages of e-commerce will be more difficult and will require a longer timeframe.\textsuperscript{98}

\textsuperscript{95} John Humphrey et al, \textit{The Reality of E-Commerce with Developing Countries} (March 2003) London School of Economics 5 < http://eprints.lse.ac.uk/3710/1/The_reality_of_e-commerce_with_developing_countries.pdf> at 10 November 2012.


\textsuperscript{97} Ibid.

\textsuperscript{98} Ibid.
E-commerce has been broadly known as a suitable model for transforming business process, but the acceptance of e-commerce has been restricted by many challenges. These challenges comprise the low level of trust in online services; lack of data protection; the poor infrastructure and a lack of the skills needed to use such infrastructure. All these factors have contributed to the limited growth of e-commerce. Other aspects that restrict e-commerce implementation in Libya include the high rates of illiteracy, low earnings per person and the lack of stable payment systems that are necessary to maintain online trading. These obstacles jointly delay the approval of e-commerce implementation in many countries or organizations.

It is crucial that these obstacles are tackled to allow e-commerce to be employed successfully. E-commerce is one of the aspects which could quickly change the base of the Libyan government strategies and enhance their online contacts’ policies; as a result, such functions will finally lead to the development of the Libyan economy.

The current situation in Libya can be summarised as following

1. customers are not deeply involved in utilising the Internet;


100 Ibid.

101 Ibid.

102 On 24 May 2012, the Former Libyan Minister of Communications and Information, Mr. Anwar Fituri and, for the government of the United Kingdom: the Minister for Trade and Investment, Stephen Green, signed a Memorandum of Intentions on e-Libya. The purpose of this Memorandum is support of the E-Libya initiative’s goals by leveraging the extensive knowledge of the UK government in the following areas

1- Information and Communication Technology (ICT) strategy;
2- Establishing a regulatory framework;
3- Physical ICT infrastructure;

103 Hamed, above n 90, 60.
2. the infrastructure of traditional commerce is being better recognised than online dealing.\textsuperscript{104}

In this new era, Libya is trying to adapt to the new technology in order to provide better living conditions to its citizens after years of difficulties. E-commerce is one of the processes through which the Libyan economy can be developed. However, there are some obstacles that impede the application of e-commerce such as the legal framework which is applicable to new technology. The Libyan economy will gain many benefits from encouraging e-commerce:

[e]-commerce will assist to build up Libya’s economy. Libya is a consumer-market, depending on imported products and as a result, consumers would save money by paying less for commodities and services. This money could be reinvested and contribute positively to the economy of the country. E-commerce may result in job cuts. However, adopting e-commerce technology will not reduce employment in Libya. Rather, it could result in creating new job opportunities and force employees to gain new skills. The importance of Libya’s location and its tourism potential will create new economic activities in the country. E-commerce would certainly help to develop the tourism industry in Libya as tourists and tour organisers were among the first to use the Internet and this has now become standard practice. Libya has many potentially attractive historical sites that could form the bases of a lucrative tourist industry.\textsuperscript{105}

As Libya begins to develop its e-commerce infrastructure, it will also have to implement a strong privacy framework. It is clear that Libya would gain many benefits from improving e-commerce facilities and accordingly, consumers should have confidence that their personal information is strictly protected by the Libyan authorities. Different surveys have revealed that privacy concerns are one of the primary reasons which obstruct e-commerce.\textsuperscript{106} It is possible that the growing of e-commerce might be linked to the trust that businesses and customers have in online transactions.\textsuperscript{107}

In January 2013, the first Libyan online website appeared under the name ‘Computer Libya’. Bensaid, the general manager of ‘Computer Libya’, said that ‘Computer

\textsuperscript{104} Ibid 62-63.

\textsuperscript{105} Ibid 277.


Libya” is one of the pioneers in B2C trade in Libya. Selling computers, printers, software and accessories, the company is running the country’s first fully-functional and exclusively online store.\(^{108}\) This means the need to establish a privacy system to protect consumers is increasing as the number of consumers who purchase online will grow in the near future.

### 2.5 Conclusion

This chapter provided the meaning of privacy according to some scholars and then moved to examine the protection of privacy in Sharia law and also some of international treaties that recognise privacy as a human right were presented. Finally, it studied the value of e-commerce in developing countries, especially Libya.

This chapter found that Sharia law, with which any legislation in Libya should comply, provides a strong safeguard for individuals’ private life and that was clear from the Quranic and prophetic texts. The Libyan authorities, in order to create a privacy system, can determine the suitable legal system without any fear that such a system might be against Sharia law because the principles of Sharia law impose no restrictions on choosing a special system of protection. The only restriction might be that when establishing a privacy system, this system should provide really strong protection to all people in the community.

Personal information that is collected by firms ‘can be used to provide better services; however, it can also be misused; for example, by sending unwanted emails to customers [and] selling customers’ information to others’.\(^{109}\) The need for a privacy system is one of the driving factors that contribute to the consumers’ confidence in online transactions. It is important that the level of trust in e-commerce is enhanced and promoted as that will lead to establishing successful e-commerce in the state. Because Libya currently has no legislation or regulation that controls or organises the area of privacy in online transactions, the aim of the next chapters will be sketching a privacy system that might be suitable to Libya.


From the research in this chapter, it is apparent that Libya privacy policy should be driven by two goals; strong protection of personal data and encouragement of e-commerce. This will require some balances as these goals will sometimes (but not always) come into conflict. In the next chapter, I examine the two main approaches to privacy self-regulation and legislative approach with this balance in mind.
Chapter III

The model of privacy protection – self-regulation or legislative approach

As discussed above, as e-commerce becomes more important, the protection of privacy in online dealings is becoming a concern for many participants in the online environment. Different countries take different approaches to addressing these concerns. For example, the European Union (EU) follows a legislative approach which takes strong steps to enforce standards and supervise the collection of personal data on the Internet. On the other hand, the United States adopts a voluntary approach to privacy in e-commerce. The appropriate model for protecting personal information within a country and among nations has been under debate. As the use of the Internet continues to increase, the threat to privacy protection also grows. This is producing substantial fears worldwide for online customer safety.

The core difference between self-regulatory and substantive legislative approaches to privacy appears to lie in differing emphases on economic growth, on the one hand, and consumer protection, on the other. The self-regulatory approach might reduce complaints and enforcement expenses; however, a legislative approach might provide greater protection for consumers. It seems that the two models of protecting personal information expose a clash between two essential values: the interest to defend individuals’ data and the need to enhance the environment of online business. In Libya, both issues of growth and consumer protection are likely to be important. This chapter examines both approaches and will argue that a substantive privacy law is more appropriate for Libya than self-regulatory approaches.

110 Gladstone, above n 80, 10.
111 Haufler, above n 107, 99.
113 Ibid.
European countries established complete data protection laws to enshrine a consumer rights-based, rather than market-based, approach to privacy. In 1981, the Council of Europe opened for signature and ratification a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which states that its objective and purpose is to

secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.

Thus, the EU attitude requires government to introduce rigorous rules to organize data transfers. However, the US approach introduces a less protective model than that in the EU because it does not consider information privacy as a basic right.

As a result of increasing concern with regard to data protection, the EU has adopted ‘rights-based’, privacy information statutes as models to protect an individual’s data. In 1998, the EU Directive 95/46 came into force, which introduced the EU principle of the basic right of data privacy. This Directive created a wide and comprehensive set of rules which provide strong protection for persons regarding the use of their private data. However, the US model attempts to rely on business principles in order to protect personal data.


120 Nijhawan, above n 117, 941.

121 Assey, above n 118, 150.
Some commentators state that the EU *Directive* identifies privacy as ‘a fundamental human right and freedom that overrides commercial concerns over regulatory costs’. Spiros Simitis said that

when we speak of data protection within the European Union, we speak of the necessity to respect the fundamental rights of the citizens. Therefore, data protection may be a subject on which you can have different answers to the various problems, but it is not a subject you can bargain about.

This chapter argues that the self-regulatory approach has some limitations which affect its efficacy. The chapter first examines the application of self-regulation in the US and illustrates how the self-regulatory model is not effective in protecting consumers. With regard to developing countries, the study then explains how developing countries lack the requirements to implement the self-regulatory approach effectively. Examples indicate such limitations are presented particularly in the area of voluntary environmental regulation and self-regulation of non-government organizations (NGOs).

The chapter argues that the legislative approach provides adequate protection to individuals and also the study explains that there is no evidence of negative impacts on economic growth if a legislative option is preferred. Finally, it argues that this approach will help to meet the requirement of adequacy as required by the EU directive. The adequacy condition requires each state that deals with the EU to provide sufficient protection to personal data. Adopting a strong privacy law will assist the State in meeting the adequacy principle to initiate business dealings between Libya and EU countries.

**3.1 Self-regulation is inappropriate choice for Libya**

Self-regulation involves each industry in specific business fields taking the responsibility for establishing its own rules and enforcing penalties, as an alternative to being managed by government entities. Thus, self-regulation as a model to protect privacy typically shows that groups of businesses create essential rules

---


123 Spiros Simitis, cited in, Ibid.

124 Gupta, above n 13, 417.
regarding gathering, using, and exchanging personal information, and also provide some measures to implement these policies in practice. One of the features of a self-regulatory approach is that it is self-enforcing, and as a consequence, online traders should build a trusted environment for business dealings as a result of the motivation that they have to encourage customers and businesses to deal with them.

The thesis argues that:

1. the self-regulatory approach has theoretical flaws which limit its effectiveness;
2. the experience of the US suggests that self-regulation has not been highly effective; and
3. the conditions for successful self-regulation are not likely to exist in developing countries.

3.1.1 Self-regulatory approach has theoretical flaws which limit its effectiveness

As a result of the increasing awareness of the exploitation and misuse of such information among consumers and their subsequent unwillingness to deal online, many companies have found that it is essential to implement privacy principles. However, the next discussion will explain that in practice, business has not offered sufficient protection to personal data.

There are some weaknesses in adopting a self-regulation approach; one of those is that companies or an industry might set up principles which do not present enough restrictions on defending personal data. Another concern in adopting a self-regulation system is that voluntary rules might be established for the benefits of the industry and not the consumers. Thus, the privacy protection of those consumers

---

126 Haufler, above n 107, 95.
might be under threat because it is not the priority of the industry. For instance, in the US, data brokers have adopted self-regulatory rules which are known as Individual Reference Services Group (IRSG) principles. These principles permit firms to sell, without restrictions, personal data to explicit subscribers, whose only obligation is to affirm their reason to access the private data of others.

Business self-regulation is not a law that has been introduced by policy-makers. Because of this, from self-regulation emerges some difficulties and challenges; for instance, the inability of public authorities to enforce the principles of data protection. Firms by themselves are expected to provide self-enforcement and self-management. One of the limitations of applying voluntary codes of conduct by businesses is not having independent supervision body to guarantee that self-regulation principles are implemented. Therefore, it is said that ‘the reluctance of many firms to include independent monitoring as an integral part of their code of conduct gives rise to some suspicion that they may be used as a public relations exercise rather than a genuine attempt at improving conditions and performance’.

The concept of free markets for privacy protection has been criticized as in this system, business will have more power and firms may use such power to abuse consumers. There are three key problems with the self-regulatory approach:

1. Privacy is an essential human right, and therefore, it should not be a bargaining matter;

---

129 Ibid.
132 Ibid.
134 Ibid.
2. Customers may find it difficult to properly estimate the market value of providing their private data; and

3. The inequity of negotiation power between consumers and business which might lead customers to lose some of their personal data if they desire to get the service.\textsuperscript{135}

The above discussion demonstrates that self-regulation is not likely to provide sufficiently strong protection to individuals as businesses commonly will defend their own benefits. The following discussion will explore the benefits that supporters of self-regulation suggest and then assess such benefits.

Advocates of self-regulation believe that industry-specific, voluntary principles and technology improvement will achieve strong privacy protection for consumers with no government intrusion. The idea is that the industry will try to defend privacy because fair dealing of private data is precious to customers, and therefore, business will try to find any possible ways to protect an individual’s data, to increase customer trust and enhance earnings.\textsuperscript{136} However, supporters of the market approach have not provided pragmatic methods by which firms can guarantee the protection of personal data. Firms can promise to protect personal data and provide strict principles but in reality, few principles are implemented.

Proponents of a free-market approach to privacy emphasise the following points to support their approach. Firstly, the damage that is caused to business by preventing free data transaction if a privacy law is enforced; secondly, the possibility of increasing costs if a consent requirement is adopted regarding data gathering and transferring and thirdly, the business’s desire to protect consumers’ privacy by tackling their concerns which is gained from the free market model as businesses take into account such concerns to defend their business growth.\textsuperscript{137}


\textsuperscript{136} Reidenberg, above n 115, 774.

\textsuperscript{137} Rubinstein, above n 125, 362.
This argument is not strong enough because it argues that if a market approach is not adopted, business will be harmed from adopting another approach to privacy. There is no model to protect privacy that aim to stop data from being transferred between nations but there are restrictive rules which determine how personal data can be gathered and used. A legislative approach does not prevent the flow of information between nations and firms but it tries to provide some restrictions on such transfers to guarantee an acceptable amount of protection.

The protection of Personal information is a human right and therefore private data should be effectively protected. Thus, the increased costs of adopting special requirements such as asking for consent from consumers should not be the primary consideration, since the priority must be the protection of personal information.

Some authors oppose the view that there is a positive effect of applying self-regulation in terms of complaints and performance because it is found that the implementation of self-regulation may provide modest links to the enhancement of a firm’s performance or compliance process, and moreover, self-regulation in some circumstances has led to diminishing a firm’s performance.138

The next discussion argues that self-regulation has not been working effectively in the US, where it has been the most developed.

3.1.2 The experience of the US suggests that self-regulation has not been highly effective

The self-regulatory approach has been adopted in the US for decades and there is clear evidence that industries and business groups have failed to provide reasonable privacy protections. The implementation of the self-regulation approach does not offer strong protection to personal data and it leads to some confusion with regard to

The voluntary system suffers generally from a lack of accountability and transparency. The conventional US assumption speculates that each firm acknowledges which suitable regulatory structure goes with its function. It is said that businesses recognise which privacy principles are appropriate to their specific field of business. On the other hand, the EU authorities are worried that such a liberal market approach may eventually encourage business groups to put their customers’ personal data into a weakly-regulated industry, which may cause that consumers’ data to be revealed without the consumers’ permission.

Some supporters of the market solution to privacy in the US claim that personal health records and sensitive financial data and children’s data have to be protected by strict rules. In addition, they argue that punishments for violating personal information should be stronger. It is interesting to observe that those who support self-regulation as an approach to protect individual data claim that enacting laws would be preferred if there is a potential of serious harm to consumers. The Vice President of the US during the Clinton presidency, Al Gore, supported the self-regulatory model but he emphasised the need to enforce legislation where sensitive data was at issue, such as children’s privacy.

In 1998, the Federal Trade Commission (FTC) in the US announced its intention to pass official regulations because groups of online businesses were unable to fully implement strict policy to protect personal information. Because the Internet is

---

139 Hoofnagle, above n 12, 1-2.
140 Rubinstein, above n 125, 356-357.
141 Nijhawan, above n 117, 964.
142 Ibid.
144 Hauffler, above n 107, 97.
145 Soma, above n 112, 185. “The Department of Commerce held a long awaited Public Meeting on Internet Privacy in June 1998, originally intended to give business an opportunity to demonstrate its self-regulatory successes. However, the industry had very little to display in terms of actual
developing and more individuals’ data is transferred without asking stakeholders’ permission, the requirement for sufficient tools for enforcement becomes a significant factor in protecting privacy.\textsuperscript{146} According to that, the FTC realised that ‘the solution must rest in another form of regulation to address privacy concerns in the United States. Several statutes have been enacted to address the key areas of financial and medical personally-identifiable information’.\textsuperscript{147}

The former Chairman of the FTC in the US, Robert Bitofsky (1995-2001), stated:

Confidence that privacy will be protected is an important element in consumers’ decisions where to shop on the Internet. Self-regulatory efforts by e-businesses to protect their customers’ privacy should be encouraged. But beyond self-regulation, those who violate consumers’ privacy should be promptly called to task. Consumers should have confidence that their privacy choices will be protected.\textsuperscript{148}

It is understood from Bitofsky’s claim that self-regulation is not working effectively to prevent violations against consumers’ data. It seems that the enforcement method is weak in forcing businesses to follow their privacy principles.

The FTC privacy framework report (\textit{Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers})\textsuperscript{149} suggests that ‘Congress consider baseline privacy legislation while industry implements the final privacy framework through individual company initiatives and through strong and achievement of privacy practices, and hence, the Secretary of Commerce approved that the business society was failing to show efficient self-regulation.’ Reidenberg, above n 115, 776.

\textsuperscript{146} Ibid.
\textsuperscript{147} Ibid. See, eg, some laws enacted in the US to protect personal data in specific area (1) \textit{Children’s Online Privacy Protection Act of 1998} (COPPA) which covers websites that are collecting information from children under the age of thirteen and which are required to comply with the FTC; (2) The \textit{Family Educational Rights and Privacy Act} (FERPA) 20 USC § 1232g is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the US Department of Education; (3) \textit{Video Privacy Protection Act} 18 USC § 2710(a)(4) which covers pre-recorded video cassette tapes or similar audio visual materials; and (4) the \textit{Fair Credit Reporting Act} covers only ‘credit reports’: \textit{Fair Credit Reporting Act} 15 USC §§ 1681a-1681x.


\textsuperscript{149} The privacy structure laid out in this Report reveals the wide evidence gained from the discussion of Commission’s privacy forums, and the received notes from more than 450 public observations as a response to the FTC proposed project revealed in 2010. See Federal Trade Commission (US), \textit{Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers}, An FTC Report (26 March, 2012) \texttt{<http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>} at 30-8-2013.
enforceable self-regulatory initiatives’.\textsuperscript{150} Maureen K Ohlhausen, who is a commissioner of the FTC, encourages the establishment of information protection law.\textsuperscript{151} As a consequence of protecting personal data from unlawful usage, Ohlhausen suggests that privacy law should give the FTC the opportunity to disseminate policies.\textsuperscript{152} Hence, it is obvious that in the US, there is real debate about the efficacy of adopting self-regulation and there is growing support for choosing data protection law as a more suitable model to protect personal information.

The former FTC Chairman Jonathan Leibowitz has stated that in fact, customers do not understand privacy rules. As a result, Leibowitz encourages businesses to adopt modern methods of privacy disclosures to gain transparency; for example, introducing a comprehensible and consistent notice system.\textsuperscript{153}

Rotenberg claims that ‘one cannot escape the conclusion that privacy policy in the United States today reflects what industry is prepared to do, rather than what the public wants done’.\textsuperscript{154} This is clear from business practice in the US where consumer concerns about control of personal data are disregarded.\textsuperscript{155} Thus, ‘self-regulation is not a genuine alternative to the legislature’s intervention. At best, self-regulation can only help to supplement legislation’.\textsuperscript{156}


\textsuperscript{151} See Jared Strauss and Kenneth S Rogerson: They state that ‘[m]any privacy advocates and legislators have argued that the US Congress should pass legislation requiring businesses to follow fair information practices as has been done in the member states of the European Union.’ Jared Strauss and Kenneth S Rogerson, ‘Policies for Online Privacy in the United States and the European Union’ (2002) 19(2) Telematics and Informatics 188.


\textsuperscript{155} The \textit{Wall Street Journal} in its feature question of the day asked the next question: Should the government require companies to only collect personal info if consumers agree, or should the marketplace decide the rules? Almost 75% of participants responded that consumer permission is necessary. Current at 28 March 2013 at <http://online.wsj.com/community/groups/question-day-229/topics/should-companies-required-only-collect>.

It is interesting to provide some examples to show how US firms do not really provide strict protection for personal data. These examples which will provide firstly the clash between Facebook and the FTC, and then the conflict between Google and the EU, show that some US companies lack adequate safeguards for the protection of personal data.

A- Facebook and the US Federal Trade Commission (FTC)

In this circumstance there was a dispute between Facebook and the FTC. The FTC claimed that Facebook had infringed the law when it engaged in misleading and unfair practices. The FTC said that Facebook failed to uphold its promise not to share users’ data with advertisers. In addition, during an update of the Facebook page in 2009, Facebook failed to inform stakeholders that the new update would release some personal information without consumer consent. Therefore, in 2011, Facebook agreed to a specific settlement, under which Facebook is

---


The FTC complaint lists a number of instances in which Facebook allegedly made promises that it did not keep:

- In December 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. They didn't warn users that this change was coming, or get their approval in advance.

- Facebook represented that third-party apps that users installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data – data the apps didn't need.

- Facebook told users they could restrict sharing of data to limited audiences – for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used.

- Facebook had a "Verified Apps" program & claimed it certified the security of participating apps. It didn't.

- Facebook promised users that it would not share their personal information with advertisers. It did.

- Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.

- Facebook claimed that it complied with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It didn't.

1. barred from making misrepresentations about the privacy or security of consumers’ personal information;

2. required to obtain consumers’ affirmative express consent before enacting changes that override their privacy preferences;

3. required to prevent anyone from accessing a user’s material more than 30 days after the user has deleted his or her account;

4. required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers’ information; and

5. required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers’ information is protected.\textsuperscript{158}

Jon Leibowtiz said that ‘Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users’.\textsuperscript{159} He claimed that ‘Facebook’s innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not’.\textsuperscript{160}

B- Google and the EU

Google is facing allegations from the EU that Google abuses its users’ personal information. As a result of such allegations, Google could face severe fines if found guilty of breaking EU law.\textsuperscript{161}

In 2012, Google introduced joint information privacy rules for all its services. This new policy permits the firm to unite data on personal users from its services, which include YouTube, Gmail and social network Google+. As result of this policy,


\textsuperscript{159} Ibid.

\textsuperscript{160} Ibid.

stakeholders have no opportunity to opt out. There are fears that Google’s new privacy policy will create a high risk to data protection. The company has been accused of gathering a huge amount of personal data on users’ online behaviours. Google keeps this kind of data for a long time and users don’t have the power to control the usage of their data. Accordingly, six European states have brought legal action against Google.

Isabelle Pierrotin, head of the French Data Protection Authority (CNIL), claims that ‘no one is against Google’s objective of simplicity. It is legitimate. But it needs to be accompanied by transparency for consumers and the ability to say yes or no’. She also said that ‘consumers have the right to know how the information is being used and what’s being done with it’. Johannes Caspar, a German data protection commissioner, said, ‘many users do not even know what is happening with their data and might worry that their private information is used to produce personality profiles of them’.

C- Evaluation

These two examples illustrate that the US firms have not provided a strict policy to protect personal data. It appears from Google’s policy that its users do not have the power to opt out or even know what is done with their personal data. This shows how industry self-regulation policy does represent strong principles to guarantee consumers protection. However, under data protection law Google would have to adhere to privacy principles as they would be part of the law. Thus, in the EU, Google has to fulfil the requirements of the EU Directive to follow principles of data protection.

162 Ibid.
163 Ibid.
165 ‘EU taskforce takes legal action against Google’ (2 April 2013) DW News <http://www.dw.de/eu-taskforce-takes-legal-action-against-google/a-16715381>, at 31-8-2013.
167 Ibid.
As the Facebook example shows, it appears that the FTC generally deals with privacy infringement case by case by suggesting negotiated settlements that would resolve the issue. Enacting data protection law, by contrast, will enforce same privacy principles on all businesses. Furthermore, by adopting national privacy principles businesses themselves may find it easier to comply with these rules. It is likely that in the Facebook case, if there were data protection laws in place, consumers would be better protected by data protection principles which would place some restrictions on Facebook regarding the collection and usage of their users’ data.

Although the FTC aims to minimise the damage that might be caused to consumers from privacy breaches, it might be better to introduce some substantive principles that are standardised across all businesses and are created by the legislative process. This could potentially improve the clarity and certainty of obligations and ensure that substantive privacy norms are created through a public and democratic process.

Companies have a strong motivation to gather large amounts of personal data because of its economic value to business; thus, supporters of the legislative model claim that governments ought to offer comprehensive laws to provide real protection for individual information.\textsuperscript{168} Enacting regulations can unite privacy principles in a country, and as a result, data protection law may reduce legal ambiguity and thus contribute to business growth.\textsuperscript{169}

From the practice of the self-regulatory model in the US, it is clear that there are many limitations on enforcing privacy principles which are adopted by businesses. Joel Reidenberg asserts that

\textsuperscript{\cite{Dennis D Hirsch, ‘The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?’ (2011) 34(2) Seattle University Law Review 452.}

\textsuperscript{\cite{Marsh, above n 114, 556.}}
In the end, self-regulation and technical tools have proven to be more public relations than meaningful information privacy for citizens. Reidenberg suggested that the United States needs a structure that offers coherent fair information principles that consider how firms deal with personal information in terms of data usage, transference and security. Reidenberg suggests that because the OECD Guiding Principles introduce inclusive privacy principles, so these standards should be adopted in law as the US structure for data protection law.

Even to the extent that self-regulation does work in the US, it is important to look at the application of business self-regulation in developing countries. The next discussion will demonstrate the practices in some developing countries which apply the self-governing approach to different fields. The experience of developing countries in these examples might offer a clear image regarding the effectiveness of the voluntary approach to regulating privacy. The next section argues that the practices of self-regulation in developing countries indicate those countries are limited in their ability to meet the requirements to apply such a model effectively. The practices of self-regulation in the area of environmental regulation and non-government organizations (NGOs) explain the limitations of applying self-regulatory approaches in developing countries.

3.1.3 The conditions for successful self-regulation are not likely to exist in developing countries

Developing countries usually do not meet the requirements which are needed to have effective self-regulation. These requirements comprise valuable legal and regulatory structures by which companies can be supervised to ensure that they follow their policies and thus take responsibility when they fail to comply with market policies, and consumer knowledge regarding their rights. If these requirements are not met, then self-regulation might be an unfavourable approach to be adopted.

---

171 Reidenberg, above n 115, 788.
172 Ibid.
Self-governing standards ‘are usually vague in terms of how they are to be measured and enforced’. When firms join industry standards, then these companies by themselves monitor the standards in operation and assess the principles. Nevertheless, few institutions are really concerned about the enforcement of their principles in practice.

This section explains that self-regulation requires special conditions which are absent in developing countries, and then shows some experiences of the self-regulatory model in developing countries in other domains.

1 **Self-regulation requires special conditions which are absent in developing countries**

Prakash Sethi suggests the following guidelines which industry self-government should meet in order to achieve its aim of effectively implementing business standards and policies:

1. In order to address consumers’ concern, the industry voluntary standards should be clear. The firm’s principles should examine matters that encompass public fears, and not just issues chosen by the business. ‘The broad principles must be amplified into objective, quantifiable, and outcome-oriented standards. These would allow for uniformity in performance evaluation and compliance assurance’.

2. Voluntary standards should be accurate in tackling matters arising during business dealings.

---


175 Ibid.


177 Ibid.
3. The firm’s standards have to be ‘realistic in the context of the industry’s financial strength and competitive environment’. The industry should not demonstrate overstated promises.

4. In order to guarantee successful compliance systems, firms have to build up a well-organized, internal, implementation arrangement.

5. A voluntary business compliance system has to be an essential element of a supervision performance assessment and incentive scheme.\(^{178}\)

6. In order to attain public confidence and reliability in the business’s performance, the external supervision and compliance authentication scheme should be established. Firms have to be under observation by independent, external monitoring to guarantee the implementation of standards in practice.

7. High transparency and disclosure of business performance to the community should be encouraged. The voluntary code of conduct should make the reports of external inspections available to the community.\(^{179}\)

These requirements for applying an effective business self-regulatory model are entirely or partially absent from the practice of self-regulation in developing counties. The practice of voluntary regulation in developing countries has shown an inability to meet such significant necessities in enforcing business principles. The lack of strong enforcement processes, complaints systems, clear standards, and transparency is observable in developing countries.

\(^{178}\) ‘For example, at the individual company level, code compliance must be integrated into the firm’s normal decision-making structure and systems. It should also have the oversight for compliance assurance at the level of corporate general counsel, and preferably with a reporting obligation to a committee of the board of directors, such as an audit committee or public policy committee. In the final analysis, the top management of the company must be held accountable for ensuring the company’s compliance with code standards’. Ibid, 12.

\(^{179}\) ‘This condition has … faced considerable resistance on the part of companies and industry groups. It is argued that releasing such reports would expose those companies to further assaults by their critics, who would not have access to similar information from other companies whose performance may be far worse’. Ibid 13-14.
To introduce effective business codes of conduct, clear tools should be implemented to make the engagement of stakeholders easier in producing industry standards, instead of just introducing these standards through companies, without any contribution from the stakeholders. In addition, ‘self-regulation needs to be in the self-interest of industry to not only occur, but also to be effective. The more incentives for businesses to make self-regulation work, then the more chance that self-regulation will be effective in achieving improved market outcomes for consumers’.  

Some factors which illustrate the limitations of self-regulation in developing countries can be demonstrated as follows:

- The lack of non-regulatory pressure and many of the non-regulatory aspects aim to encourage companies to operate effectively with self-regulation. These non-regulatory factors include demands from customers, non-governmental organizations and community groups, but these factors are apparently weak in developing countries.
- The lack of regulatory pressure in developing countries: mandatory directives are often a significant incentive for corporations to join in and conform to self-regulatory schemes.
- In developing countries, agendas and regulatory procedures are commonly influenced what will benefit the firms.

The implementation of self-regulation in developing countries might be unsuccessful because there are many obstacles as discussed above. It is not easy to adopt self-regulation due to the weakness of the legal and regulations framework, the lack of

---

180 Jenkins, above n 133, 29.


‘The Australian Food and Grocery Council commented that the strongest incentive for industry to ensure that self-regulation is effective is the imperative of the industry, as whole and individual companies, to protect their reputations in the marketplace. It submitted that once a self-regulatory measure is established, and promoted by the industry as a commitment to a set of values and a desire to meet the needs of consumers, individual companies and the industry as a whole will strive to meet the benchmarks it has set.’ Ibid.

enforcement in developing countries as firms do not intend to apply their policies, and the weaknesses of the compliance mechanisms which should force firms to take responsibility for their wrongdoings.  

It is important to discuss one of the most obvious limitations to applying self-regulation in developing countries, which is the lack of non-regulatory pressure. A study which examined the self-regulatory model as applied to environmental regulation in developing countries found that an apparent barrier for the spread of such an approach in emerging economies is associated with the weakness of companies’ abilities. Pressures from non-government organizations (NGOs) and consumers groups are responsible for enhancing firms’ ability to apply their standards because pressure from stakeholders can lead firms to develop and improve their performance. However, this pressure is absent or weak in developing countries.

(i) Consumers’ behaviour in developing countries

Consumer knowledge regarding their interests is considered to be vital in adopting self-regulation because consumers can increase pressure on businesses to follow their policy and take more responsibility. However, the consumer pressure in developing country is not strong enough to force firms to respect customers’ rights. It is said that, with regard to consumer knowledge about collecting and transferring their personal data,

> [w]eb users are often unaware of the collection of their personal information online, as much of it occurs instantaneously and invisibly. Even where they are aware of the collection of personal data, users often do not understand how network advertisers and data brokers will combine this information with other data about them; how employers, lenders, and others will use these profiles; and

---

183 Azmat, above n 173, 8-9.
185 Ibid 139.
186 Blackman, above n 182.
187 Azmat, above n 173, 6.
how data mining operations can infer additional, latent information from such data.\textsuperscript{188}

The role of consumer participation in the standardisation process has been analysed in the developing countries. From such analysis, it has been indicated that the inadequate participation of consumers in the standardisation process might be connected to the lack of consumer interest groups or NGOs whose main goal should be to address consumers’ concern.\textsuperscript{189} In a comparison between consumers in developing countries and consumers in developed countries, it is noticeable that consumers in emerging economies have gained less education. For instance, with regard to the environmental circumstances, consumers in developing countries have no clear concerns about environmental issues.\textsuperscript{190} It might be possible to draw a similar inference with respect to privacy that consumers might not be able to value their privacy.

The United Nations (UN) provides *Guidelines for Consumer Protection* which especially suggests guidelines for consumer protection in developing countries. The UN programme encourages governments to play a vital role in developing and supporting the growth of consumer education which includes information about consumer behaviour and the expected benefits and costs of changes in utilisation.\textsuperscript{191} The goal of these educational programmes is to allow consumers to understand and be aware of their rights and duties and also to be able of being free in making decisions with regard to their options of commodities and services.\textsuperscript{192}

\begin{flushleft}
\textsuperscript{188} Hirsch, above n 168, 455.
\end{flushleft}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\textsuperscript{192} Ibid.
\end{flushleft}
In a study that analysed the view of consumers in four developing countries, it was found that respondents who participate in such studies prefer that governments play a vital role by introducing regulations for solving consumer issues.\footnote{William K Darley and Denise M Johnson, ‘Cross-National Comparison of Consumer Attitudes toward Consumerism in Four Developing Countries’ (1993) 27(1) \textit{Journal of Consumer Affairs} 50.}

It is clear that consumers in developing economies are suffering from a lack of knowledge regarding their rights and obligations and such limitations are considered to affect their choices. Because consumer pressure is a significant element in implementing effective self-regulation, when such a factor is absent, the implementation of a self-regulatory model will not be effective in developing countries.

2 The practice of the self-regulatory model in developing countries

The following examples from developing countries will provide a picture of how self-regulation is not working effectively in such countries. These practices will be in two areas: firstly, voluntary environmental regulation and secondly, the regulation of NGOs. These two cases provide an indication that because these two fields have suffered from many limitations, it is predicted that self-regulation as a model to protect privacy will suffer from the same limitations, as the problems are likely to be systemic in developing countries.

A - Voluntary Environmental Regulation

Developed countries have recognised self-regulation for decades and it has been popular as a tool to control pollution.\footnote{Allen Blackman et al, ‘Voluntary Environmental Regulation in Developing Countries: Mexico’s Clean Industry Program’ (2010) 60(3) \textit{Journal of Environmental Economics and Management} 182-183.} In developing countries, environmental administrations have adopted some voluntary codes for environmental protection guidelines. For instance, a great number of voluntary agreements concerning environmental protection by companies have been adopted in some countries in Latin America such as Colombia and Chile.\footnote{Ibid.} Nevertheless, modest data is available about the state of self-regulation in developing countries to recognise what factors lead
firms to participate in such voluntary proposals and whether adopting a self-management approach will improve their environmental protection operations.\textsuperscript{196}

Consumer concerns are considered as one of the motivations to adopt self-regulation in environmental management protection.\textsuperscript{197} A number of studies have confirmed that businesses commonly agreed to environmental supervision principles because these firms were under pressure from customers to ensure environmental protection. A Canadian study showed that consumer pressure was the second factor that leads companies to follow environmental protection guidelines (government pressure was the first factor in adopting such environmental protection programmes).\textsuperscript{198}

It is clear that groups such as consumer organizations or environmental safeguard advocates play a vital role in the area of environmental protection and thus, in order to perform, they may carry out direct, lawful action against companies that do not respect their principles. It is assumed that stakeholders have the motivation to commence an action which might affect a lot of institutions.\textsuperscript{199} The issue in developing countries, as discussed earlier, is that consumer knowledge is weak and those stakeholders are not educated enough to recognise their rights and accordingly, to force firms to follow their environmental principles.

The effectiveness of environmental preservation is under criticism in the circumstance of adopting voluntary rules because it has been argued that firms’ motivation to adopt such voluntary principles are reducing government regulations and hiding weak environmental operations.\textsuperscript{200}

A study which has examined the implementation of the self-regulatory method in Costa Rica will be explored by considering the efficacy of such practice.

\textsuperscript{196} Ibid.
\textsuperscript{198} Ibid.
(i)- The Costa Rican practice

An example of environmental voluntary regulation can be drawn from the Costa Rican approach. As a result of growing concern about environmental issues in the tourism sector, the Costa Rican Ministry of Tourism created, in 1997, the Certification for Sustainable Tourism (CST) program for hotels. This programme is thought to be the initial self-governing environmental system established by a developing country authority.\textsuperscript{201} The Costa Rican initiative intended to improve compliance in environmental issues which was believed to be significant to a large number of customers who were considered as ‘green’ consumers.\textsuperscript{202}

A study by Rivera examined the effectiveness of voluntary environmental initiative in the Developing World. The study was built on data gathered from surveys and records from a sample of 164 Costa Rican hotels. This study recognised two groups; the initial one included Costa Rican hotels which were enrolled in the CST Program (about 52 hotels in 1999). The other group of 112 hotels was derived from a random review of 250 hotels.\textsuperscript{203}

The study showed that hotels which engaged in the CST system had different reasons to do so. A number of hotels tended to conceal their weak environmental attitude and thus evaded increased attention from supervisors and environmental advocates. Also, other hotels might gain ‘green’ reputations with no clear enhancements to their environmental operation.\textsuperscript{204}

In this study which examined the Costa Rican approach of adopting environmental self-regulation in operating Costa Rican hotels, it found that fewer than ten percent of hotels in the country adopted a voluntary programme to maintain environmental

\textsuperscript{201} Ibid 335.
\textsuperscript{202} ‘The CST program was designed in partnership with leading academic institutions, the major hotel trade association, environmental organizations, and hotel managers. Representatives of these groups are also members of the independent National Accreditation Commission that regulates the CST standards and supervises the hotel certification process’. Ibid 335-336.
\textsuperscript{203} Ibid 342.
\textsuperscript{204} Ibid 347.
protection and the majority among those hotels proved to have a small degree of adherence to environmental protection.205

**B- Self-regulation of Non-Government Organizations (NGOs) in developing countries**

Similarly, self-regulation of NGOs in developing countries has not been effective. It has been explained above that special requirements are needed in order to have an effective self-regulation practice. The following example will indicate how the self-regulation approach as a method of organising NGOs has not been strong in developing countries.206

**(i)- Kenyan NGOs’ practice**

The first country to be examined is Kenya which was the first in all African countries to build up a regime of self-regulation. The system is controlled by the Kenyan National Council of NGOs, which has the legal right to organise NGOs in the country.207

The Kenyan NGO Code of Practice includes seven principles; one of these standards is a complaint scheme which permits any person to lodge a case against any participants in NGO self-regulation if there is any infringement of the Code of Conduct and this complaint scheme provides the process regarding how to lodge a complaint. In the circumstance where an NGO violates the Kenyan Code of Conduct, the Regulatory Committee may enforce sanctions against that institution.208

---

205 It has been said that ‘[a]lthough these results cannot be generalized beyond Costa Rica, promoters of the CST program in other countries can learn from this evidence. For instance, it would not be unreasonable to expect even lower levels of enrolment and environmental performance in countries that: (1) lack a significant segment of ‘green’ consumers, (2) fail to show minimum government oversight, (3) have less cooperative policy networks, or (4) lack organized hotel industry associations.’ Ibid 355.

206 In a study which focused on NGOs in Africa, statistics and information were gathered for analysing the effectiveness of NGOs in Kenya and Ethiopia and such data contains interviews with 30 leading directors and programme personnel of NGOs, contributors and government administrations. Thus, it appears that this study would be valuable to show the effectiveness of self-regulation in developing countries. Mary Kay Gugerty, ‘The Effectiveness of NGO Self-regulation: Theory and Evidence from Africa’ (2008) 28 (2) Public Administration and Development 112.

207 Ibid.

208 Ibid.
Nevertheless, the Kenyan regime of self-regulation has some disadvantages: one of drawbacks is that the Code of Practice principles are broad, and thus, standards are not clear. As a result of such wide rules, it is not easy to identify what is required by the regulations.\textsuperscript{209} The council membership expresses little information with regard to NGO value and it is not clear whether NGOs are well-informed on their commitment to the Code of Practice. The enforcement system is really fragile because there is no clear method regarding the complaints process and the system is built on public complaints procedures, but there is no indication that the public actually has any knowledge about their rights and the process for carrying out a case against NGOs.\textsuperscript{210}

(ii) Botswana NGOs’ practice

The second example is the Botswana Code of Conduct, produced in 2001, under the sponsorship of the Botswana Council of NGOs. The national strategy supposes that the Code will be applied to all NGOs in Botswana; however, a strict provision which requires NGOs in Botswana to sign on and to adhere to the Code is absent.\textsuperscript{211}

The principles set out in the self-regulation Code of Practice are broad guidelines which include values such as transparency and liability. However, ‘NGOs are expected to monitor their own adherence to the code. There are neither reporting requirements for NGOs, nor any provisions for monitoring by [Botswana Council of NGOs].'\textsuperscript{212}

As happened in Kenya, the system has suffered from many weaknesses and that is clear from the lack of enforcement system. It has been noticed in this approach that there is no supervisory authority for the Botswana Council of NGOs. It is unclear how to lodge complaints or how conflicts with the Code would be investigated. There is a lack of regulatory ability because the Code of Practice is considered too broad.\textsuperscript{213}

\textsuperscript{209} Ibid 112.
\textsuperscript{210} Ibid.
\textsuperscript{211} Ibid 114.
\textsuperscript{212} Ibid.
\textsuperscript{213} Ibid.
These examples from Africa give an indication that developing countries are lacking the specific requirements that are vital in order to adopt effective self-regulation. Some commentators have found that the self-governing approach as a method to enforce standards in developed countries might not be applicable to the context of developing countries because possibly these rules are applied in dissimilar ‘socio-political’ circumstances.214

3. Conclusion for Libya

In order to be implemented successfully, self-regulation needs particular terms of enforcement, transparency, and observation measures.215 Supervision is a central feature of self-regulation to make sure that businesses standards have been implemented effectively.216 Creating a self-regulatory proposal is not the only requirement for implementation; in addition, business has to take responsibility to guarantee that self-regulation is achieving its goals.217

Furthermore, transparency is considered to be a significant element to have effective self-regulation because consumers may not have enough understanding about some technical issues which might prevent consumers from protecting themselves. Clear principles would be an important instrument to guarantee reliability and responsibility.218

The experience of self-regulation in developing countries which has been provided in this chapter has suggested that the implementation of industry self-governance may not be strong enough to defend personal data. It is noticed that many obstacles face the application of self-regulation to protect stakeholders in particular fields of business. For instance, the lack of transparency and enforcement both provide real challenges to implementing the voluntary approach in developing countries and it is believed that the protection of privacy by industry rules would not be an exception.

214 Blackman, above n 194, 182-183.
216 Commonwealth of Australia Department of the Treasury, above n 181, 78.
217 Ibid.
218 Ibid 71.
Currently, Libya is one of those developing countries that may face similar challenges to countries in this category. The public awareness in adopting self-regulation is considered as an important element in order to have an effective self-governing system, but achieving this in developing countries is not easy as it requires consumers to understand their rights and to know how to complain when their rights have been challenged by others. Moreover, the enforcement method in the self-regulatory approach is not obvious and therefore there is no apparent mechanism to force firms or organizations to implement their policy. This limitation may demonstrate that the self-regulation method of privacy protection is not favoured for adoption in Libya. Given the importance of privacy as a human right, self-regulation does not seem to be appropriate in the Libyan context.

The next discussion will examine the reasons that support the choice of the legislative approach regarding the protection of privacy in Libya.

3.2 Legislative approach is the suitable model for Libya

This section will argue that legislative model to privacy is a preferred model in order to guarantee strong protection to personal information. It will argue that Law provides adequate protection to individuals. Then it will illustrate that Legislative approach does not show negative impacts on business growth. Finally, in order to deal with the EU, legislative approach would be the suitable choice.

3.2.1 Law provides adequate protection to individuals

The legislative approach affirms that direct, government legislation adds confidence to consumers and as a result, contribute to economic growth. The implementation of a governmental model to control a particular part of business is vital in many ways:

1- A public authority has the opportunity to properly predict the cost of regulation and thus establish rules which consider such a significant matter.

---

219 Peng Hwa Ang, above n 15, 3.

220 See Prakash and Potoski, above n 21, 775.
2- Public administration has the capability to force businesses to abide by regulations and implement policies in a State. 221

3- Legislation applies to all firms or industries if they fall under the category of law. Hence, there is no opportunity for businesses to ignore the application of legislation. 222

4- The legislative approach might have the ability to accomplish its aim which may be difficult to gain through self-governing options. 223

These benefits which may be gained from introducing legislation for an extensive privacy law are likely to be an imperative element to adopt the legislation model for privacy. Indeed, implementing the legislative approach resolves two issues that may be caused by choosing the self-regulatory as model for privacy: firstly, the lack of motivation to offer real data protection and secondly, the weakness of enforcement mechanisms and particularly penalties. 224

However, supporters of less regulation have considered that data protection law might negatively affect business:

1. Enforcing regulations might slow down the progress of the market. It is argued that if the government entity has little knowledge about the business that it aims to regulate, such a regulation might impose burdensome conditions, which may badly harm the industry’s competitive environment. 225

2. A government might find it difficult to adapt its law to the emerging new technology which makes legislation out of date and unable to achieve its goals. 227

221 Ibid.
222 National Consumer Council (UK), above n 22, 18.
223 Ibid.
224 Strauss, above n 151, 188.
225 Ibid.
226 An example that has been provided is ‘a statute requiring firms to post large and eye-catching notices about their data collection practices, designed for delivery to computer screens, will not fit on the mobile phone screens through which more and more people now access the Internet. Such rules will seriously constrain innovation or become obsolete as technologies and business practices change.’ See Hirsch, above n 168, 454.
227 Hirsch, above n 168, 454.
3. Also, enforcing legislation regarding data protection might increase the cost of providing services, and therefore, negatively affect industry innovation.\textsuperscript{228}

Some commentators assert that the legislative attitude toward privacy protection might be a solution to privacy issues.\textsuperscript{229} However, an inadequately drafted Act may negatively affect innovation.\textsuperscript{230} Therefore, any data protection law should not only provide protection to consumers, but also should not harm the practice of business as far as is possible.

As a response to these drawbacks of the governmental model, many solutions could be provided. Firstly, to tackle the issue of introducing an inadequately drafted Act, policy-makers should have enough knowledge about the effect of enforcing new privacy principles. In order to accomplish that, lawmakers in a country should gain help from legal advisers who have experience in the area of regulation and should also consider the views of businesses to draft the most suitable privacy law.

Secondly, every law, over time, will need to be amended and data protection laws are no exception; thus, there should be a committee that aims to evaluate the operation of the laws and suggest any changes to be made to the Act.

Business’s failure to protect consumers by way of self-governing rules has contributed to the increase in government controls, as a consequence of demands to widen principles of performance in industry.\textsuperscript{231} The governmental approach is seen as a tool which embraces powerful and efficient regulation; this is the effect of one government entity taking responsibility for the performance of the regulations. Therefore, government entities have a wider jurisdiction and supremacy than self-regulatory organizations.\textsuperscript{232} The role of government might be significant in the data

\textsuperscript{228} Haufler, above n 107, 103.

\textsuperscript{229} Marsh, above n 114, 558.

\textsuperscript{230} Ibid.


\textsuperscript{232} Ibid 18.
protection area which comprises standards clarification, registering data gathering, and resolving clashes.\textsuperscript{233}

The practice in Europe demonstrates the value of establishing privacy law because in the EU, privacy is considered a basic ‘democratic value’, for which adequate protection should be offered by a legal framework.\textsuperscript{234} Data protection in Europe is a significant area of established protection. The EU Directive, as a result, attempted to lay down high, comprehensive principles with regard to securing personal information. The EU Directive introduces an international form of an accurate law-making model for data protection law.\textsuperscript{235} The data protection law should be precise, deliberate, and harmonious to achieve its aim, which is protecting personal data.\textsuperscript{236}

According to the European model for privacy protection, the EU Directive ensures that a great number of rights are guaranteed such as the protection of civilians and the sensible treatment of personal information. Commonly, the EU data protection approach recognises all individuals with their fundamental right to their data.\textsuperscript{237} Thus, European citizens have the power to organise the gathering and utilising of their data. Firms or industry not only have to follow the process of the EU Directive which organises the gaining, storing, using, and disclosing of individuals’ data, but also they should ensure that individuals have the authority to access stored data and to correct errors.\textsuperscript{238} Additionally, each plan should help individuals to keep control over their data by giving them information considering who collects their data and

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{233}] Fred H Cate, *Privacy in the Information Age* (Brookings Institute Press, Washington D.C. 1997) 121.
\item[\textsuperscript{234}] Joel R Reidenberg, ‘Should the U.S. Adopt European-Style Data-Privacy Protections?’ *The Wall Street Journal* (8 March 2013) <http://online.wsj.com/article/SB10001424127887324338604578328393797127094.html?mod=WSJ_article_comments#articleTabs%3DArticle> at 20-8-2013.
\item[\textsuperscript{236}] Cate, above n 233, 109.
\item[\textsuperscript{237}] Reidenberg, above n 115, 782.
\item[\textsuperscript{238}] See EU Directive 95/46/EC and EU Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature 28 January 1981, CETS No 108 (entered into force 1 October 1985).
\end{itemize}
\end{footnotesize}
how to access their data and by asking for permission and consent for the gathering or movement of data.\textsuperscript{239}

Paul Schwartz said that there is a need for the adopted approach of privacy to allocate different roles to the legislature, judiciary, and supervisory agencies, and not just grant individuals the right to privacy.\textsuperscript{240} Schwartz states some elements that are considered as vital for establishing a legal system that exemplifies the importance of data protection rules:

1. legislation should describe requirements for dealing with personal information with respect to the usage of personal data;
2. the establishment of comprehensive principles should be understood by customers for transparency and also for consumers to know all the transactions with their data. Individuals should be given the power to deal with their rights by being informed about the transactions with their personal information; and
3. the introducing of a government entity for supervising the way in which personal data is being stored or used.\textsuperscript{241}

These elements are very important in order to have an effective data protection law because when principles of new law describes the requirements and obligations with regard to data usage or storage, such obligations will give consumers the confidence they need to purchase online. Furthermore, if data protection standards are clear enough, that will ensure that any customers will decide correctly what they really want from their actions and not be misled or subjected to deceptive conduct. Finally, to implement a new law effectively, there is a need for an external body that supervises companies and revises their privacy standards to determine whether data protection principles are applied according to the law or not.


\textsuperscript{241} Ibid.
3.2.2 Legislative approach does not show evidence of negative impacts on business growth

Gaining the trust of consumers could possibly be one of the vital elements for successful business brand names.242 One of the main sources of economic growth in internet commerce is establishing confidence in online trading. Thus, failing to reach the necessary level of consumer trust may lead customers to be reluctant to purchase online. Losing such confidence in the online environment may negatively affect the progress of innovation.

The idea that data protection law will negatively impact on economic growth and innovations has not been strong enough to prevent policy-makers from adopting privacy laws in the majority of countries that provide protection to personal data. The European Commission considered information protection to be the vital element in supporting the proposal of the Digital Agenda for EU (DAE).243 This DAE proposal ‘intends to help Europe’s citizens, businesses and improve Europe’s financial system and to receive great benefits from using new tools of technology’.244 The DAE is the ‘first of seven flagships initiatives under Europe 2020, the EU’s strategy to deliver smart sustainable and inclusive growth’.245 It seems that producing data protection law can contribute to the enhancement of economic growth and prosperity for citizens.

Joel Reidenberg argues that

[s]tricter privacy laws don’t stifle innovation or prevent online companies from sending targeted offers to consumers. Rather, they shift control from industry to individuals by requiring businesses to demonstrate that consumers approve of the way their information is being used.246

242 Haufler, above n 107, 99.
245 Ibid.
246 Reidenberg, above n 234.
This argument clearly indicates the role of data protection law in a society because privacy law manages or organises the possible ways in which personal data is collected or stored, and therefore, firms will not lose the ability to use individuals’ data but individuals will have the power over their information as they should be given information about how their data is being transferred or stored by companies.

Companies may promote the introduction of data protection law, when this law enforces rational obligations on business and ensures adequate protection for consumers’ data.247 Two of the large online firms- Microsoft Corp and Google Inc - have supported the view that Congress ought to take action by enacting comprehensive privacy law to offer enough protection with regard to collecting and using consumers’ information.248

At a Senate Commerce Committee hearing on online advertising, Google and Microsoft claimed that significant privacy rules ought to be built on three central values: Firstly, customers should evidently be notified about what type of personal data is gathered about them; secondly, the public has the right to organize how their information is used; and finally, personal data should be secured to guarantee that personal information is not misused by others.249 Such a movement from these big firms gives an indication that introducing data protection law will help them manage their users’ data and make sure that such data is secured. Furthermore, it will be understood that firms will not be harmed by enacting a data protection law because such legislation will contribute to fixing any confusion related to the matter of dealing with personal information.

The Irish Minister for Justice and Equality, Alan Shatter, stated that, with regard to the new proposal of EU data protection law,

>[t]he new Data Protection package is an essential tool for enhancing confidence in the online marketplace. The proposals aim to improve individual’s control of their personal data, including the “right to be forgotten”, whereby an individual no longer wants his or her information processed on the internet. This new right


249 Ibid.
will go some way to address the possible reputational, financial and psychological risks associated with social networking and internet based sites.\textsuperscript{250} Some European representatives suggest that the EU needs a strong governmental agenda within which citizens will be under protection but which will also permit businesses to receive the benefits of Europe’s digital market.\textsuperscript{251} The views of the EU representatives reflect the notion that data protection law will have many benefits for the economies of European countries. ‘In 2011, the European market had a value of €3.5 billion for software products and €1.1 billion for hardware products. Estimates for 2014 predict that this market will grow to €11 billion’.\textsuperscript{252} It is estimated that with the growing number of online consumers - around 500 million - EU GDP could grow by approximately 4% by 2020 when the EU forms an up-to-date structure of the digital environment.\textsuperscript{253}

In a comparison between the percentages of consumers buying online in 2011 and the estimated percentages in 2016 for different EU countries, it seems that there is an increase in such percentages: France: 63%, 76%; Germany: 69%, 81%; Italy: 36%, 47%; Netherlands: 75%, 85%; Spain: 41%, 58%; Sweden: 72%, 86%; U.K.: 75%, 85%.\textsuperscript{254} Viviane Reding and Alan Shatter, with regard to the new proposal of EU data protection law, suggested that the proposed EU data protection improvements will help business to innovate and contribute to growth:

\textsuperscript{252} Ibid.
\textsuperscript{253} Ibid.
1- It will decrease expenses and increase legal confidence when replacing the present mess of laws in Europe with an identical set of principles for all EU countries.

2- As infringements of data protection law can cause huge damage to business, firms will consider the necessity of data protection safeguards to diminish the threat. When consumers have enough knowledge regarding their data, more customers will purchase on the internet and that will have a good impact on business growth.

3- The new rules can offer transparency for global data transfers. ‘The new EU data protection rules will improve the current system of binding corporate rules to make these types of exchanges less burdensome and more secure.’\textsuperscript{255}

It is clear that introducing data protection law has not been overly burdensome on business because it appears that in the EU countries, there is an indication of growth in the number of consumers who are dealing online which will lead to business growth.

Some may argue that if there is no data protection law in the EU, then the EU industries might gain more profits. On the whole, however, the evidence suggests that the impact of privacy regulation on growth appears to be minimal. States should therefore be able to develop a privacy law that strikes an appropriate balance between the requirements of growth and protection for fundamental individual rights.

Therefore, enacting privacy law will guarantee that consumers have enough protection regarding their individual data and also businesses know their obligations regarding data gathering or storing. Industry’s profits might be less when there is data protection law but in order to balance the consumers’ right to control their data and the businesses’ ability to gain benefits, the law would be the best option for balance between the two groups (consumers and businesses).

\textbf{3.2.3 Data protection law in Libya in order to deal with the EU}

The EU Directive has had noteworthy effects in that it has contributed to the growth of the EU form of protecting personal information, and it has contributed to the

\textsuperscript{255} Reding and Shatter above n 251.
establishment of several regulations within and outside the European region. For instance, some countries have implemented new privacy regulations specifically in order to maintain business dealings with the EU.

The EU Directive on Data Protection which went into effect in October of 1998, prohibits the transfer of personal data to non-European Union countries that do not meet the EU ‘adequacy’ principles of protection personal information. As a result of differences between US approach and EU approach, the US Department of Commerce has signed an agreement with the EU that allows associations to join a Safe Harbor List to reveal their fulfilment of the European Union Data Protection Directive. Because of such agreement, data can be transferred between the EU and the US firms which follow the Safe Harbor List.

It is understood that any country outside the EU should have adequate protection of personal information in order to receive data from the EU. Therefore, Libya, in order to have a trade relationship with the EU, should demonstrate that it provides

---


258 The EU Directive 95/46/EC ‘Transfer Of Personal Data To Third Countries’, art 25


The US-EU Safe Harbor agenda offers a number of significant benefits to US and EU associations. Advantages for US businesses joining such a programme include:

1- All 28 Member States of the European Union will be bound by the European Commission’s finding of “adequacy”;

2- Participating organizations will be deemed to provide “adequate” privacy protection;

3- Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted;

4- Claims brought by EU citizens against U.S. organizations will be heard, subject to limited exceptions, in the U.S.; and

5- Compliance requirements are streamlined and cost-effective, which should particularly benefit small and medium enterprises.

EU businesses will make sure that it is sending data to a US organization which follows the US-EU Safe Harbor platform. This can be gained by looking at the list which contains the names of all US organizations that have joined the Safe Harbor programme.

sufficient protection for personal information. The best option for Libya is to adopt a legislative approach for data protection as this model will entail comprehensive standards and consequently, will provide much stronger safeguards for private information.

In November 2008, the EU and Libya started talks about a Trade Agreement. The goal was to formulate an agreement which covers trade in goods, services and investment, but because of the Libyan uprising in early 2011, the EU-Libya negotiations were suspended in February 2011. Prior to the negotiations’ suspension, the talks led to the writing of a draft agreement between Libya and the EU. It is interesting to note how that draft considered the matter of privacy protection.

The EU-Libya draft framework agreement, art 42, under the title, ‘Data Processing’, stipulates that

1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier;

2. Each Party, reaffirming its commitment to protect fundamental rights and freedom of individuals shall adopt adequate safeguards to protect privacy, in particular with regard to the transfer of personal data.

It has been explained in this draft framework that for greater certainty, this commitment (to protect fundamental rights and freedom of individuals shall adopt adequate safeguards to protect privacy) indicates the rights and freedoms as set out in

---

260 In 2010, before the Arab Spring and the uprising in Libya, ‘the EU was an important trading partner for Libya accounting for 70% of the country’s total trade, which amounted to approximately €35.5 billion in 2010. The EU was Libya’s major source of imports and its largest market for exports in 2010’. See EU Commission: Trade <http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/countries/libya/ > at 1-9-2013.


the *Universal Declaration of Human Rights*, the UN *Guidelines for the Regulation of Computerised Personal Data Files* (UN General Assembly Resolution 45/95 of 14 December 1990), and the OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (adopted by the Council on 23 September 1980).

Securing compliance with EU regulations is determined on a case-by-case basis. In order to ensure that Libyan organisations can engage in trading relationships with EU entities, it will be important for Libya to adopt a strong privacy framework. The EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data claims that ‘it is clear that any meaningful analysis of adequate

---

263 The UN General Assembly attempted to recognise the importance of providing the minimum principles to deal with computerized personal data. Thus, on 14 December 1990, the UN General Assembly adopted Resolution 45/95 which provided Guidelines for the Regulation of Personal Data Files. These guidelines contain procedures for implementing regulations concerning computerized personal data files. The procedures for implementing regulations concerning computerized personal data files are left to the initiative of each State. The guidelines stipulate principles concerning the minimum guarantees that should be provided in national legislations. These principles are

1. Principle of lawfulness and fairness;
2. Principle of accuracy;
3. Principle of the purpose-specification;
4. Principle of interested-person access;
5. Principle of non-discrimination;
6. Power to make exceptions;
7. Principle of security;
8. Supervision and sanctions;
9. Trans-border data flows;
10. Field of application.

*Guidelines for the Regulation of Computerized Personal Data Files*, UN doc 45/95 (14 December 1990).


The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application’. 266

Under the EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data, at a minimum, Libya must consider the basic rules applicable on dealing with personal data and the mechanisms for guaranteeing their effectual implementation.

266 Ibid. Under art 29 of EU Directive 95/46 EC the Working Party on the Protection of Individuals with regard to the Processing of Personal Data was established. The working party has advisory status and acts independently. Article 30 of EU Directive 95/46 EC stipulates that

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.
With regard to basic principles, the Working Party suggest the following principles:

1) the purpose limitation principle;
2) the data quality and proportionality;
3) the transparency;
4) the security principle;
5) the rights of access, rectification and opposition; and
6) restrictions on onward transfers.\footnote{267}

With regard to Procedural/Enforcement Mechanisms, the working party states that:

to provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries.

The objectives of a data protection system are essentially threefold:

1) to deliver a good level of compliance with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

2) to provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

3) to provide appropriate redress to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.\footnote{268}

It appears that \textit{EU Directive} requires a minimum protection to personal data in a country that will receive data from the EU. Thus, generally, it is important to the countries that want to commence a trade with the EU to provide sufficient protection to personal data.

The next two chapters will examine in detail the basic principles of dealing with personal data and the enforcement mechanisms which are needed to enforce the law effectively. It is clear that any future privacy law in Libya should take into

\footnote{267}Ibid 6.
\footnote{268}Ibid 7.
considerations the objective of data protection law that introduced by the EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data. This thesis in next two chapters will make sure that such requirements are met.

3.3 Conclusion

This chapter argued that the self-regulation approach is not an effective model for providing sufficient protection for an individual’s data. The practice of such an approach in the US and also in developing countries was discussed. In order to provide strong protection for personal data, this chapter demonstrated that the legislative approach as a model to protect personal data is the appropriate option for Libya.

Sharia law is the main source of legislation in Libya as the Libyan Constitutional Declaration provides. Therefore, any new legislation must comply with Islamic standards, and any law which contradicts Sharia principles will be held to be unconstitutional. As has been discussed in a previous chapter, Sharia law principles provide strict rules to guarantee the protection of an individual’s privacy in a society. Because Sharia law principles perceive the right to protect privacy as a fundamental human right, it seems that Sharia law supports the legislative approach, as this approach provides a complete and adequate framework regarding using, storing and collecting personal data.

For reasons explained in this chapter which support the legislative approach to privacy protection, it seems that legislation as a model to protect personal information from misuse is a suitable approach that Libya should pursue. Therefore, it is suggested that Libya should, in the near future, consider the value of introducing a privacy law. This law should be encouraged by policy-makers, consumer groups

---

269 See the Libyan Constitutional Declaration (2011) Art 1.

270 See how Sharia principles respect the right to individuals’ privacy explained in ch 2 above.

271 Spiros Simitis claims that ‘[o]mnibus laws were since the earliest days of data protection, especially in Europe, considered to be the only means to secure both a broad and reliable way to regulate the use of personal data’. Simitis, above n 156, 2000.
and businesses. The law ought to have comprehensive and clear principles in order to provide transparency with the transformation of private information.
Chapter IV

Data protection Law

It has been concluded in Chapter 3 that substantive data protection legal regime is the most suitable option for the Libyan context as it is more likely to provide sufficient protection to the processing of personal information. In general, the principles of the EU Directive can be used as a guideline to form data protection law in Libya. The EU practice shows a strong consideration of the protection of personal information and the evidence indicates that the protection of personal information in the EU region is stronger compared to other districts. However, certain matters must be considered to guarantee that the law is suitable for the Libyan context. In particular, the guidelines usually point out the general principles and leave details to the national laws to set up. Thus, the Libyan policy-makers can make their own decision about how the principles will be implemented in practice.

To determine the extent of the application of data protection law is essential to identify where it would be implemented and where it would not. Enforcing legislation means that obligations, rights and penalties would be stipulated, and thus, to recognise which circumstances will be covered by the law is important for the strength and effectiveness of the rules. In order to understand the scope of data protection law, some terms should be defined to give a clear image regarding the application of the law.

The most important part of data protection law is fair information principles which consider the requirements regarding the treatment of individuals’ data. The fair information principles require specific procedures before processing personal data; for example, the notice requirement stipulates that data controllers provide notice to data subjects regarding the purpose of processing their personal information. It is clear that these principles should be identified and explained as it is considered to be the basis of any data protection law.

In order to discuss and evaluate the scope and principles of data protection law, different data protection laws will be examined to learn from their practice and to avoid the same obstacles that these laws have faced. These laws will be presented to consider their directions in particular areas of privacy concerns. The laws include the Data Protection Act 1998 (UK), the Privacy Act 1988 (Cth), the Personal Data Protection Act 2010 (Malaysia). In addition, the approach of the EU Directive 95/46 EC and the OECD Guidelines (2013) will be presented.

4.1 The scope of data protection law

To recognise the circumstances under which data protection law should be applied, it is required firstly to provide the general direction adopted by different jurisdictions to get a comprehensive understanding of the scope and secondly, to define some linked technical terms to clarify the scope. Finally, some exceptions from the application of data protection law which have been implemented by some different legislation will be studied to decide whether they might be adopted with regard to the Libyan context.

4.1.1 The extent of the application of data protection law

This section discusses the capacity of data protection law and under which circumstances data protection law might be applicable. This will be done by examining the practice of different data protection laws.

Commonly, data protection law does not cover some parts of privacy; for example, privacy related to the body. There is apparent agreement that data protection law applies to the processing of personal data and that can be seen from the practice of different data protection laws. Personal information protection acts usually apply to protect individuals whose privacy is under threat when their information is processed by data controllers.


274 Ibid. Data Protection Act 1998 (UK) s 5 stipulates that:

(1) Except as otherwise provided by or under section 54, this Act applies to a data controller in respect of any data only if—
Regarding its scope, the EU Directive states that\textsuperscript{275}:

\textit{This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.}\textsuperscript{276}

The EU Directive provides the scope of data protection law by stating that the directive is applied on the processing of personal data. The EU Directive defined processing of personal data as follows:

‘Processing’ shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.\textsuperscript{277}

The EU Directive expands the application of the Directive to include many ways of dealing with personal data such as the collection, recording and storage of individuals’ information.

\begin{itemize}
\item[(a)] the data controller is established in the United Kingdom and the data are processed in the context of that establishment, or
\item[(b)] the data controller is established neither in the United Kingdom nor in any other EEA State but uses equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom.
\end{itemize}

(2) A data controller falling within subsection (1)(b) must nominate for the purposes of this Act a representative established in the United Kingdom.

(3) For the purposes of subsections (1) and (2), each of the following is to be treated as established in the United Kingdom—
\begin{itemize}
\item[(a)] an individual who is ordinarily resident in the United Kingdom,
\item[(b)] a body incorporated under the law of, or of any part of, the United Kingdom,
\item[(c)] a partnership or other unincorporated association formed under the law of any part of the United Kingdom, and
\item[(d)] any person who does not fall within paragraph (a), (b) or (c) but maintains in the United Kingdom—
\begin{itemize}
\item[(i)] an office, branch or agency through which he carries on any activity, or
\item[(ii)] a regular practice;
\end{itemize}
\end{itemize}

and the reference to establishment in any other EEA State has a corresponding meaning.

\textsuperscript{275} The EU Directive 95/46/EC, art 3.

\textsuperscript{276} The EU Directive 95/46/EC art 2 defined:

\begin{itemize}
\item[(c)] ‘personal data filing system’ (‘filing system’) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
\end{itemize}

\textsuperscript{277} The EU Directive 95/46/EC art 2(b).
Similarly, the Malaysian Personal Data Protection Act 2010 applies to the processing of personal data by data controllers.\textsuperscript{278} It stipulates that:

2. (1) This Act applies to

(a) any person who processes; and

(b) any person who has control over or authorizes the processing of,

any personal data in respect of commercial transactions.\textsuperscript{279}

The Personal Information Protection and Electronic Documents Act 2000 (Canada) states that data protection law applies to the processing of personal information. The law stipulates that:

This Part applies to every organization in respect of personal information that

(a) the organization collects, uses or discloses in the course of commercial activities.\textsuperscript{280}

It is obvious from the scope of data protection whether in the EU Directive, the Malaysian Act or the Canadian Act, that the main focus is on personal information which is processed by data controllers. Data protection law applies to protect the processing of personal information and thus personal information should be defined in order to gain a clear understanding of the scope of any relevant law. The next subsection will define this and other important terms.

4.1.2 Identifying some terms in order to clarify the scope

The above subsection explained the area that data protection law should cover, but to get a clear understanding of the scope of the law, some of the terms which are pivotal to understanding the scope and principles of data protection law should be defined. Also, with regard to some terms, the forthcoming discussion indicates that there are

\textsuperscript{278} ‘After close to a decade, the Personal Data Protection Act (PDPA) was finally passed in April 2010, an Act which was initially intended to be part of the Malaysian government’s regulatory framework known as the Malaysian Cyber Laws designed to support the Multimedia Super Corridor (MSC) project’. Rebecca Ong, ‘Data Protection in Malaysia and Hong Kong: One Step Forward, Two Steps Back?’ (2012) 28(4) Computer Law and Security Review.

\textsuperscript{279} Personal Data Protection Act 2010 (Malaysia) art 2. This law has not come into force yet at 6 August 2013.

\textsuperscript{280} Personal Information Protection and Electronic Documents Act SC 2000 (Canada) s 4.
different approaches which define such terms, and thus some choices need to be made. The meaning of personal information, sensitive data, data controllers, data subjects and finally, data processors, is considered below.

1- Personal Information

Personal information is generally defined as data that relates to an individual.

Article 2 (a) of the EU directive 95/46 EC stipulates that

> personal data shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.  

The Malaysian law defines personal data as follows:

> ‘Personal data’ means any information in respect of commercial transactions, which

(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject.

The Data Protection Act 1998 (UK) states that

> ‘Personal data’ means data which relate to a living individual who can be identified

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

---

281 The term ‘personal data’ used in EU Directive 95/46 ‘undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies.’ Lindqvist [2003] (C-101/01) European Court Report I-12971 at 24.

282 Personal Data Protection Act 2010 (Malaysia) art 4.
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.\textsuperscript{283}

It is understood from these definitions that personal information includes data that relates to an individual. The expansion of the definition of personal data by including any information related to individual may, in fact, provide stringent protection for personal information. This broad approach seems appropriate because it may guarantee that a huge amount of data would be considered as personal information if it was related to or linked to individuals, and therefore would be covered by data protection law and accordingly would be treated under the principles of fair information practices.\textsuperscript{284}

The OECD Guidelines suggest that ‘personal data convey information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person’.\textsuperscript{285}

\begin{center}
\textbf{Recommendation 4.1: a broad approach to defining personal data should be adopted.}
\end{center}

The next discussion will examine two issues that relate to the meaning of personal information. The first issue is that the law is only applied to protect natural persons and the second issue is that the law is implemented only to protecting living persons.

\textsuperscript{283} Data Protection Act 1998 (UK) s 1(1).

\textsuperscript{284} See the Australian Law Reform Commission which states that the current definition of ‘personal information’ in Australia contains the following elements:
• information or an opinion;
• including information or an opinion forming part of a database;
• whether true or not;
• whether recorded in a material form or not;
• about an individual;
• whose identity is apparent from the information or opinion; or
• whose identity can reasonably be ascertained from the information or opinion.

A- Natural person

Because privacy is a human right and this right is mainly concerned with a physical person, data protection law should generally be implemented for a natural person and not a corporation. If there is any threat to corporate information, other sections of law shall be applicable, not privacy law. For example, commercial law may set out some protection for legal persons.

This approach was endorsed by the Australian Law Reform Commission (the ‘ALRC’). The Australian Law Reform Commission argues that art 17 of the International Covenant on Civil and Political Rights only applies to the reputation, honour and the protection of personal data. The practice of the international approach to this issue reflects that, in many jurisdictions, data protection Acts do not apply to corporations or organisations (non-natural persons).

This approach is consistent across a number of different regions. The EU Directive also limits the definition of personal information to information about natural persons only. Similarly, the OECD Guidelines explained that the definition of personal data is applied only to natural persons. The OECD explanatory memorandum about the protection of privacy guideline claims that

[they]he Guidelines reflect the view that the notions of individual integrity and privacy are in many respects particular and should not be treated the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another. Some members of the Expert Group suggested that the possibility of extending the Guidelines to legal persons (corporations, associations) should be provided for. This suggestion has not secured a sufficient consensus. The scope of the Guidelines is therefore confined to data relating to individuals.


287 Ibid.

288 The EU Directive 95/46 EC art 2(a).


290 Ibid [33].
Recommendation 4.2: data protection Act should apply to natural persons and should not apply to corporations or organisations.

B- Living individuals

The other issue to be considered about the scope of data protection law is the extent to which restrictions extend to deceased persons.

It is valuable to note that Data Protection Act 1998 (UK) states that information should be related to a living person. The UK Information Commission office states that data protection law in the UK is applicable only to the living person; thus, when the data subject of personal information is lifeless, the information linked to the dead person cannot be personal information. The EU Directive and Malaysian law do not address this issue.

With regard to including deceased persons in the definitions of personal data, the ALRC supports the view that data protection law should comprise some sections that treat, in specific circumstances, the use of the individual data of dead persons.

The ALRC states that

[the ALRC does not believe, however, that it is appropriate simply to extend the definition of ‘personal information’ in the Act to include the personal information of deceased individuals. It is clear that not all the privacy principles can be applied sensibly, or applied in full, to the personal information of deceased individuals. Instead, the Privacy Act should be amended to make specific provision for dealing with the personal information of deceased individuals.]

To extend the definition of personal information to include deceased persons might cause some difficulties in practice. Particularly, some data protection principles may be applicable only to living persons. However, the approach of the ALRC to apply

---

293 Ibid.
294 Australian Law Reform Commission, above n 284, 226.
specific provisions regarding the protection of dead persons might help to ease this issue.

The Libyan legislators, when they come to enact privacy law, should take into account the issue of dead individuals. Data protection law may include the protection of personal information of deceased persons in special circumstances where disclosure may affect the interests of other persons. For example, the relatives of deceased persons may ask for protection in specific circumstances if they could be harmed by the revelation of the deceased’s personal information.

<table>
<thead>
<tr>
<th>Recommendation 4.3: data protection law should be applicable only to living persons, but the law may include the protection of deceased persons in exceptional circumstances.</th>
</tr>
</thead>
</table>

2- Data subject

It is vital to recognise the data subject because the individual whose data is being processed by data controllers should be identified, as this person is considered as the subject of data protection law. A data subject is defined as a person whose data would be acquired and accessed by data controllers.295

The UK Data Protection Act 1998 defined data subject as ‘an individual who is the subject of personal data’.296 The Malaysian Act adopts the same definition which stipulates that ‘[d]ata subject means an individual who is the subject of the personal data’.297

According to the UK data protection law, ‘a data subject must be a living individual. Organisations, such as companies and other corporate and unincorporated bodies of persons cannot, therefore, be data subjects’.298

---

296 Data Protection Act 1998 (UK) s 1(e).
297 Personal Data Protection Act 2010 (Malaysia) art 4, Interpretation.
298 Information Commissioner’s Office (UK), above n 291, 16.
As discussed earlier, personal information shall not include information related to legal persons such as corporations and associations, thus, only a natural person would be a data subject. However, a dead person might be a data subject under some circumstances which data protection law may provide for.\textsuperscript{299}

**Recommendation 4.4: the definition of ‘data subject’ should include a natural person and in some circumstances might include a deceased person.**

### 3- Sensitive data

Most States divide personal data into two categories: general personal data, and sensitive personal data. Sensitive personal data is protected to a greater degree because of its greater importance. In implementing a Libyan privacy framework, attention must be paid to whether different levels of protection are required for different types of data.

The Malaysian privacy law defines ‘sensitive personal data’ to mean

\[\text{any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence.}\]

Information that is linked to descent or ethnic origin, political or religious beliefs, for example, is very much personal. Such these data is not often required and it is needed by some associations in only some situations.\textsuperscript{301}

The Canadian *Personal Information Protection and Electronic Documents Act 2000* asserts that, with regard to determining sensitive personal data, although

\[\text{[s]ome information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.}\]

\textsuperscript{299} See this chapter 4.1.2 (1) definition of personal information.

\textsuperscript{300} *Personal Data Protection Act 2010* (Malaysia) art 4.

\textsuperscript{301} Australian Law Reform Commission, above n 284, 208.

\textsuperscript{302} *Personal Information Protection and Electronic Documents Act SC 2000* c5, sch 1.
However, the Australian Law Reform Commission adopts a different direction in order to define sensitive data by claiming that

[p]ersonal information can become more or less sensitive because of the context in which it is considered and notes that this can apply to almost any personal information. The ALRC is not of the view, however, that the definition of ‘sensitive information’ should be amended to include information made sensitive by context. On balance, the existing approach of listing categories of information as sensitive provides greater certainty.303

There are apparently two methods to distinguish normal personal data from sensitive personal data; the one adopted by Canadian law may suggest more protection to a wide range of data depending on the circumstances. As such, sensitive information will be determined depending on the context; for instance, what might be considered sensitive in one situation could be determined not sensitive in another circumstance. Because sensitive data will be dealt with under strict rules, expanding the definition of sensitive data by linking personal information to the context might provide a real and greater protection to individuals.

If the method of adopting specific categories of sensitive personal data is chosen, such an approach might provide less protection to individuals because there might be some situations where some data which should be considered as sensitive will not, because it is not included under specific categories.

While adopting an approach which defines sensitive data by listing categories of information as sensitive achieves some clarity, adopting a border approach to define sensitive data may lead to expand the protection of individuals which will be defined according to the context. Since the primary consideration of this thesis is on providing a strong protection of personal data, this suggests that adopting broad definitions of sensitive personal data may be preferred. Thus, the Libyan policy-makers, when they come to consider this issue, may prefer to consider personal information as sensitive depending on the context for which such information was disclosed. Sensitive data shall be treated by strict rules because this type of information might cause great harm to individuals if not treated with specific protective safeguards.

303 Australian Law Reform Commission, above n 284, 213.
Recommendation 4.5: Sensitive information should be determined depending on the context and not on listing categories of information as sensitive.

4- Data controller

As data controllers are required to meet the terms of the data protection principles, it is vital to define ‘data controllers’. The UK Data Protection Act 1998 provides that

[i]t shall be the duty of a data controller to comply with the Data Protection Principles in relation to all personal data with respect to which he is the data controller.

The EU Directive defined data controller to mean

the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

Similarly, the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013) and Malaysian law define data controllers. The OECD defines data controller to mean

a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.

The Malaysian Personal Data Protection Act 2010 defined data user (controller) to mean

a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor.

304 Information Commissioner’s Office (UK), above n 291, 16.
305 Data Protection Act 1998 (UK) s 4(4).
308 Personal Data Protection Act 2010 (Malaysia).
It is notable that the Malaysian law states that a data controller is a person. The legal definition of ‘person’ is:

1) A human being.

2) A corporation treated as having the rights and obligations of a person. Counties and cities can be treated as a person in the same manner as a corporation.\textsuperscript{309}

Therefore, data controller could be a natural person or a legal person such as an organisation which deals with personal information.\textsuperscript{310} The word ‘person’ ‘comprises not only individuals but also organisations such as companies and other corporate and unincorporated bodies of persons’.\textsuperscript{311} The Malaysian law states that data controller means a person and under the legal definition, a person will include a natural person or an organisation.

The definition of the EU Directive might be preferred because it clearly defines data controllers to comprise natural and legal persons, public authorities and agents. This broad definition widens the application and enforcement of data protection law. Thus, data controller should mean the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes of the processing of personal data.

**Recommendation 4.6: the definition of ‘data controller’ should include the natural or legal person, public authority or any other body.**

5- Data processor

‘Data processor’ should be clearly defined as data protection laws might stipulate some requirements for the way data processors treat personal information. ‘Data processor’ could be a person who process data on behalf of a data controller.\textsuperscript{312}


\textsuperscript{310} The EU Directive 95/46 EC art 2.

\textsuperscript{311} Information Commissioner’s Office (UK), above n 291, 16.

\textsuperscript{312} Stead, above n 295, 9.
The Malaysian *Personal Data Protection Act 2010* defines ‘data processor’, in relation to personal data to mean

any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.\(^\text{313}\)

The *EU Directive* provides that ‘processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller’.\(^\text{314}\)

**Recommendation 4.7: the definition of ‘data processor’ should include a natural or legal person and public authority which transact personal data on behalf of data controller.**

From this clarification of the scope of data protection law, it should now be possible to identify some exceptions to this scope. These exceptions are provided by different jurisdictions. The next subsection will evaluate such exceptions and which exceptions should be adopted in Libya.

### 4.1.3 Exceptions to the scope of data protection law

The scope of data protection law is usually applied to the processing of personal information and some restrictions will be enforced in order to provide a clear protection to individuals’ data. However, some legal systems have suggested some limitations on the scope of data protection law for different reasons. The exceptions that will be examined in this chapter are family and household affairs; public or private sector; non-commercial transitions; small business exceptions; national security and defence, and finally, other exceptions.

Thus, the next discussion will evaluate the significant of such exceptions and in particular, in the Libyan context.

---

\(^{313}\) *Personal Data Protection Act 2010* (Malaysia) art 4.

\(^{314}\) The *EU Directive* 95/46 EC art 2 e.
4.1.3.1 Family or household affairs

Many data protection laws in different regions state that data protection Acts should not be applicable to natural persons in the course of individual activity. The Australian Privacy Act 1988 (Cth) under title ‘Personal, family or household affairs’ takes this direction by providing that

[n]othing in the National Privacy Principles applies to:

(a) the collection, holding, use, disclosure or transfer of personal information by an individual; or

(b) personal information held by an individual;

only for the purposes of, or in connection with, his or her personal, family or household affairs.\(^{315}\)

Similarly, the EU Directive takes the same approach by stipulating that the Directive shall not apply to the processing of personal data ‘by a natural person in the course of a purely personal or household activity’.\(^{316}\)

In addition, the UK Data Protection Act 1998, under the title ‘Domestic purposes’, recognises the exception of family and household affairs from the application of data protection law. The UK law requires that

[p]ersonal data processed by an individual only for the purposes of that individual’s personal, family or household affairs (including recreational purposes) are exempt from the data protection principles.\(^{317}\)

Many data protection laws recognise the exception of processing an individual’s data in the course of private or family affairs from the application of data protection legislation. Libyan authorities may consider this issue and they might accept the view that data protection law should adopt the exception of family and personal affairs from the law’s application. This exception could be accepted because it is not predicted that the same principles of dealing with personal data that are enforced on

---

\(^{315}\) Privacy Act1988 (Cth) s 16 E. Jeremy Douglas-Stewart gives an example for such a circumstance. It is explained that if Peter is an IT manager at a hospital, and Peter’s mother asks him to gather her medical records from the hospital. As such, it is not required that Peter complied with the Privacy Act because such activity would be regarded as a family affair. Jeremy Douglas-Stewart, Annotated National Privacy Principles (Presidian Legal Publications, 4th ed, Adelaide, 2009).

\(^{316}\) The EU Directive 95/46 EC art 3.

\(^{317}\) Data Protection Act 1998 (UK), s 36.
data controllers will apply to the family and household affairs. Family relationships present the circumstances that personal data could be transferred without the requirement of giving notice or providing security measures.

**Recommendation 4.8: family and personal affairs should be excluded from data protection law.**

### 4.1.3.2 Public or private entities

There are different directions regarding whether data protection law is applicable to the private sector as well as the public sector. Some data protection laws exclude the public sector from the law’s application, however others enforce data protection law on both the public and private sectors.

There is also an argument that legislation should only apply to public sector because government deals with most important personal information. To argue that government databases deal with most important personal information and therefore, privacy law should only apply to governments entities is not strong because just as the personal data of individuals that is processed by governments needs strong protection, personal data that is processed by firms also needs strong protection. There should be no difference in the protection of personal data depending on the controllers of such information. As the protection of personal data is a fundamental human right, the protection of personal data should be offered, whether this data is stored by government or firms. Firms also deal with vital and sensitive information related to specific individuals and such information must be protected, as well as the information controlled by government entities.

There has been some suggestion that governments introducing privacy regulation should gain experience in regulating the public sector first, and then implement the law on private entities. Given that it is important to protect information gathered by both private and public sector organisations, delaying protection for the private sector is not likely to be a desirable option because:

---


319 Ibid.
1. government may take a long time until it can gain such experience;

2. government’s priority should be to offer enough protection to personal data whether this data is gathered by government bodies or private firms; and

3. privacy is considered a human right and therefore, legislation should be enacted as soon as possible to give an indication that the country respects personal data and enforces strong rules to defend personal information, without regard to who collects and processes the personal data.

By contrast, Malaysian data protection law takes the approach that federal government and state governments will be excluded from the law’s implementation. Section 3 of the Malaysian Personal Data Protection Act 2010 (‘PDPA’) under the title, ‘Non- application’ stipulates that ‘[t]his Act shall not apply to the Federal Government and State Governments’.\textsuperscript{320} According to such exclusion, Federal government will be excluded from the provisions of the Malaysian Personal Data Protection Act. It is suggested that the law will exempt regional offices and state divisions or bureaus that have relation with the state government.\textsuperscript{321} Such a limitation from the law’s application may have a huge effect because excluding government entities will be harmful as the public sector, through its different offices such as the immigration sectors, is one of the largest collectors and users of personal data in the country.\textsuperscript{322}

Rebecca Ong argues, with regard to providing such an exception to Malaysian personal data protection law, that

\[\text{[i]t is doubtful whether the exclusion of the public sector is prudent and accords with the objective of the data privacy law. This raises the question whether instead of safeguarding the interests of data subjects, the PDPA was enacted to legitimise the data-processing practices of the government.}\textsuperscript{323}\]

Data protection law should be implemented on private and public sectors because the protection of personal data must be the priority of any law. If government entities are

\textsuperscript{320} Personal Data Protection Act 2010 (Malaysia) s 3(1).
\textsuperscript{321} Ong, above n 278, 432-433.
\textsuperscript{322} Ibid.
\textsuperscript{323} Ibid.
excluded from the application of the law, that may lead to unbalanced dealings between the government and the data subject. Government would have strong power over personal information without clear procedures about how the protection of individuals’ data is guaranteed, if the government, as data controller, is excluded from data protection law.

Abu Bakar Munir, with regard to the Malaysian exclusion of the public sector from the application of the Data Protection Act, states that ‘[i]t is acceptable to have a separate regime for private and public sectors which is on par with each other. But having a law that applies only to the private sector is not ideal and not in line with international norms’. 324 Graham Greenleaf claims that the Malaysian law ‘can only be said to cover part of the private sector, and only then subject to many exceptions, particularly where any State-related activities are concerned. Within its scope it may still be valuable, but the narrow scope must always be kept in mind’. 325

Moreover, data protection law should be applied to private firms because these firms are collecting and dealing with a great amount of personal data, and data protection principles that are embodied in legislation will control how firms will deal with personal information.

Recommendation 4.9: data protection obligations should be implemented on public and private sectors.

4.1.3.3 Exception of non-commercial transactions

This exception is stipulating that only personal information accessed in the course of a commercial transaction would be subject to the application of data protection law. Article 2 of the Malaysian Personal Data Protection Act 2010 limits the application of the law to ‘commercial transactions’ and would exclude non-commercial


organizations, educational associations and non-profit organizations’. The Malaysian Personal Data Protection Act 2010 defined ‘commercial’ to mean any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.

With regard to such limitations, there is a strong weakness in introducing such a limitation to privacy law.

It has been accepted that this may pose difficulties since it is not easy to draw a line between a commercial transaction and a non-commercial transaction, for example, a person who participates in a fund-raising event organised by a charitable organization or a survey conducted by an educational institution. Personal information is a valuable commodity whether or not it is processed by an organization or an individual in pursuant of a commercial transaction or otherwise. It is difficult to comprehend why such a distinction should be made before protection can be afforded to a data subject.

Such a distinction between commercial and non-commercial transactions may not comply with the object of data protection law which supposes that the protection of personal data should be the priority of any law. Therefore, any data protection law should concentrate on the protection of individuals whether their data is processed for commercial or non-commercial reasons.

**Recommendation 4.10:** data protection law should be implemented on the processing of personal information accessed in the course of commercial and non-commercial transactions.

### 4.1.3.4 Small business exception

This exception means that data protection law will not be applicable to small business which usually is defined by some articles in privacy law. The reason for such an exception might be to encourage small businesses to perform effectively as they will not face the high cost of compliance with privacy laws.

---

326 Ibid.
327 Personal Data Protection Act 2010 (Malaysia), art 4.
328 Ong, above n 278, 433.
Malaysian law does not provide the ‘small business exemption’, which has been provided in some jurisdictions like Australia. The Australian Privacy Principles are applied to bodies that are defined as an ‘organization’. ‘An organization is defined as an individual, a body corporate, a partnership, any other unincorporated association or a trust that is not exempt from the operation of the Privacy Act’. Specific bodies are particularly excluded from the classification of ‘organization’ and, therefore, are exempt from the Act. Australian law excludes small businesses from the definition of ‘organization’ under s 6C of the Privacy Act 1988 (Cth).

This exception of excluding small business from the application of privacy law has been under debate. On the one hand, opponents of the small business exception in Australia demonstrate some major concerns which favour the removal of the exception:

- there are no appropriate criteria that could exempt only those small businesses that pose a low risk to privacy, because any definition of ‘small business’ would be arbitrary;
- removing the exemption would reduce inconsistency and fragmentation in privacy regulation;
- removing the exemption would facilitate trade with the EU; and


330 Greenleaf, above n 325.
331 Australian Law Reform Commission, above n 284, 880.
332 Ibid.
333 Privacy Act 1988 (Cth) s 6D: Small business and small business operators: What is a small business?

(1) A business is a small business at a time (the test time) in a financial year (the current year) if its annual turnover for the previous financial year is $3,000,000 or less.

Test for new business

(2) However, if there was no time in the previous financial year when the business was carried on, the business is a small business at the test time only if its annual turnover for the current year is $3,000,000 or less.

What is a small business operator?

(3) A small business operator is an individual, body corporate, partnership, unincorporated association or trust that:

(a) carries on one or more small businesses; and
(b) does not carry on a business that is not a small business.
some small businesses, especially those in high-risk sectors, handle large amounts of personal information and carry out some of the most privacy-intrusive activities.\textsuperscript{334}

On the other hand, advocates of the small business exception argue that by retaining such an exception

- a small business may not reflect great damage to personal data protection as small firms do not gather a huge amount of private information or treat individuals’ data improperly; and

- If there is no small business exception, small firms might not be able to afford the compliance costs. It is concerned that if privacy act does not recognise the importance of such exception, the law might require strict obligations on such small companies which lead to negatively affect their operation.\textsuperscript{335}

The Australian Law Reform Commission does not believe that the small business exemption is essential or reasonable for business. It said that the high cost of compliance does not represent a strong argument to support such an exemption. In addition, it argues that similar jurisdictions abroad, for example, the UK, Canada and New Zealand, do not have a similar exemption for small businesses.\textsuperscript{336}

The small business exclusion from the law’s application is probably not ideal. As small businesses comprise a large part of the private sector their exclusion from the scope of data protection law might result in a law to be enforced on a small number of organizations which deal with personal information while a great number of firms will be free to deal with personal data without any real restrictions. Therefore, it is suggested that the Libyan authorities do not provide such an exception in data protection law.


\textsuperscript{335} Ibid.

\textsuperscript{336} Australian Law Reform Commission, above n 284, 1036.

The Government of South Australia submitted that business efficacy is not likely to be enhanced by misuse or careless management of personal information. It considered that the benefits of removing the exemption would include: enhancing the protection of personal information; clarifying consumers’ confusion and closing off loopholes under the exemption, thus promoting public confidence in the effectiveness of the privacy regime; creating a level playing field for all small businesses. Ibid 1022.
In addition, because the protection of personal information is a fundamental human right, there should not be any distinction between big or small firms who collect personal data. As the ALRC suggests, the impact of compliance on small business is unlikely to be prohibitive.

**Recommendation 4.11: data protection law should not exclude small businesses from the law’s application.**

### 4.1.3.5 Defence and National security

Most privacy legislation provides exceptions from the application of privacy law for reasons of defence and national security.

It is essential to balance the security of personal data with the protection of State security. This need is compliant with international principles that offer exceptions from privacy standards in order to protect national security. The EU Directive takes this approach when it excludes public security, defence and State security (including the economic well-being of the State when the processing operation relates to State security matters).

Furthermore, the UK Data Protection Act 1998 provides a similar provision which stipulates that

> personal data are exempt from any of the provisions of the data protection principles, if the exemption from that provision is required for the purpose of safeguarding national security.

Accordingly, the OECD Guidelines, when it comes to consider the scope of Guidelines, stipulates that

> exceptions to these Guidelines, including those relating to national sovereignty, national security and public policy (“ordre public”), should be:

a) as few as possible, and

b) made known to the public.

---

337 Ibid 922.
338 The EU Directive 95/46/EC, art 3.
These exceptions can be valuable because national sovereignty and defence should have priority over data protection. However, clear procedures should be available in order to balance personal data protection and the security of the country. A judicial review might be one of the options to determine whether, in specific circumstances, national security will have priority over personal data protection principles.

The Libyan authorities may adopt such an exception and follow the international directions as the protection of national security is considered pivotal to any nation. However, this exception should be narrow in scope and the public should be aware of the conditions of applying such an exception.

**Recommendation 4.12: privacy law should provide exceptions from the application of the law for reasons of defence and national security.**

4.1.3.6 Other exceptions

Some data protection laws may provide the opportunity to enforce more exceptions to the application of data protection law. This power might be given to special committees or to specific minister.

The Malaysian *Personal Data Protection Act* stipulates in s 46:

Power to make further exemptions

1. The Minister may, upon the recommendation of the Commissioner, by order published in the *Gazette* exempt

   (a) the application of any of the Personal Data Protection Principles under this Act to any data user or class of data users; or

   (b) any data user or class of data users from all or any of the provisions of this Act.

2. The Minister may impose any terms or conditions as he thinks fit in respect of any exemption made under subsection (1).

3. The Minister may at any time, on the recommendation of the Commissioner, by order published in the *Gazette*, revoke any order made under subsection (1).

---

It is clear that a Malaysian minister has the authority to make further exceptions from the provision of data privacy law. This power may reduce the law’s supremacy because the minister, under a recommendation from a commission, can add any exceptions. Respect for the rule of law implies that only legislators should have the power to amend the law and there are limited circumstances under which others should be given such a power. It appears that the right of Malaysian ministers to add exceptions clashes with the objective of data protection law as the minister has the authority to exclude any data user from being bound by the provisions of Malaysian law.

The Libyan legislators might not guarantee the right to provide new exclusions to any committee or minister because such an opportunity may offer strong powers to external bodies such as big firms or government agencies that might lobby for new exceptions for their benefit only.

**Recommendation 4.13:** privacy law should not give any committees or ministers the power to provide new exception to the law.

### 4.1.3.7 Conclusion

With regard to the Libyan context, a few exceptions may be introduced when they are considered vital, especially with regard to security and defence reasons. However, the law should be broad in scope and applicable to many situations because introducing many exceptions will reduce the efficacy of the law and lead to a fragile law that cannot achieve its objectives. Data protection law has to be clear in terms of words and standards in order to be successful in providing strong protection for individuals’ data.
In order to deal with the processing of personal data, data controllers have to follow some obligations. Such principles are known as ‘fair information principles’ which guarantee the consumers’ right to secure their data.

4.2 Fair information principles (Privacy principles)

Fair information principles are focused on the protection of personal data. These principles do not consider the protection of persons themselves but instead focus on the protection of personal information about individuals.  

Consumers generally have concerns, initially, about how firms or business use their personal data; secondly, fears caused when someone’s personal data might be attacked and others might get access to his or her private information. The aim of fair information principles in such circumstances is to ‘balance the competing business and consumer interests around the use of the consumer’s personal information and serve as the basis for privacy laws’.  

Data protection principles are a number of rules which are produced to describe essential rules about how data can be gathered, processed, and used. Consumers get real benefits from fair information standards because these principles are types of rules which guarantee the stakeholders the right to organise their personal data. Also, these principles are considered to be a kind of international principles for the moral exercise of dealing with individuals’ data.

The Privacy Act of 1974, 5 USC § 552a is considered as one of the first pieces of legislation among privacy laws that endorsed the fair information principles. These

341 Roger Clarke, above n 318, s 2.4.
345 Culnan and Milberg, above n 342, 11.
principles stipulate the rights of data subjects and data controllers (US citizens as data subject, and the government as data controller). 346 The purpose of the *Privacy Act of 1974*, 5 USC § 552a is to offer assured protection for individuals when there is an invasion of personal privacy, by requiring the US federal agencies to

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of wilful or intentional action which violates any individual’s rights under this Act. 347

These basic principles of fair information principles which are endorsed in the *Privacy Act of 1974*, 5 USC § 552a have played a significant role in the improvement of global guiding principles for privacy protection. 348 One of these guidelines is the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980). 349 In 2013, the *OECD* introduced revised Guidelines which govern the Protection of Privacy and Transborder Flows of Personal Data. 350

346 Rotenberg, above n 154, [42].


348 Rotenberg, above n 154, [44].

349 Ibid.

350 This revision leaves intact the original ‘Basic Principles’ of the Guidelines. See the revised Guidelines on <http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines> at 15 September 2013.
The enforcing of fair information principles through data protection law will positively affect companies’ privacy standards as they will be forced to follow privacy principles and, as a consequence, will lead to increase companies’ interest in enhancing their performance.\footnote{351}{Paul Schwartz, ‘Privacy and Democracy in Cyberspace’ (1999) 52 Vanderbilt Law Review 1697.} As such, it is said that ‘fair information principles are the building blocks of modern information privacy law’.\footnote{352}{Ibid 1614.} The current data protection laws are based on the principles of fair information principles and these standards comprise extensive principles which provide substantive and technical values such as data quality, access data and consent.\footnote{353}{Culnan and Milberg, above n 342, 11.}

It is claimed that at the core of data protection principles are four standards which involve choice, notice, access and data supervision.\footnote{354}{Ibid.} In the circumstances where personal information is gathered by data controllers, customers should know the reason for such collection, the probable uses, the possible action that would be put in place to defend personal data as a method to increase privacy and transparency, and any remedy accessible to persons.\footnote{355}{Joel R Reidenberg, ‘Setting Standards for Fair Information Practice in the US Private Sector’ (1995) 80(3) Iowa Law Review 497–498.}

Joel Reidenberg asserts that, with regard to the scope of fair principles in a society,

\begin{quote}
[s]tandards allocate both economic benefits and burdens. Politically, adequate standards for the treatment of personal information are a necessary condition for citizen participation in a democracy. Since ancient Greece, a citizen’s right to participate in society has depended on the ability to control the disclosure of personal information. Without appropriate standards, citizens may be unduly constrained in their interactions with society. Socially, the treatment of personal information is an element of basic human dignity. Fair treatment of personal information accords respect to an individual’s personality.
\end{quote}

Reidenberg explains the importance of standards in a society and how fair personal information principles can have a vital impact on citizens and such principles lead
persons to join a democratic society. Thus, clear and strong privacy principles should be encouraged in order to protect and respect personal data.

A number of international organizations and regional commissions have introduced standards regarding data protection principles such as the OECD and the EU. The OECD introduced Privacy Guidelines which are built upon the fair information principles.\textsuperscript{357} The \textit{OECD Guidelines} contain eight basic principles.\textsuperscript{358} The OECD standards summarize essential principles with regard to the free exchange of data between nations and the protection of personal information.\textsuperscript{359}

The EU \textit{Directive} 95/46 EC of data protection provides general standards and specific principles. The \textit{Directive} provides a set of rules which considers a progression of data protection principles which have been clarified by a Working Party on the Protection of Individuals with regard to the Processing of Personal Data.\textsuperscript{360}

This section will examine data protection principles which control and organise the way in which data controllers deal with personal information. The principles have been drawn from the \textit{EU Directive} and \textit{OECD Guidelines}. In fact, most data protection laws provide similar restrictions in the processing of personal data. The principles which will be explained in this section are: data quality principles; the rights of access and rectification and opposition; purpose specifications and limitation principles; the requirement of consent; the security principle; enforcement and accountability principles, and finally, restrictions on onward transfers.

\textbf{4.2.1 The data quality principle}

Most data protection laws endorse some requirements for the processing of personal data that should be taken into account by data controllers in order to gain access to

\begin{flushleft}
\textsuperscript{357} Bellman, above n 257, 314.


\textsuperscript{360} Cate, above n 353, 350.
\end{flushleft}
personal data. These obligations take into consideration the quality of personal data that will be transferred to others.

The EU *Data Protection Directive* places some obligations on data controllers which the users of personal data have to follow when transferring individuals’ data.\(^{361}\) The EU *Directive* states that private data must be

1. processed fairly and lawfully;\(^{362}\)
2. collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
3. adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
4. accurate and, where necessary, kept up to date; and
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.\(^{363}\)

Similarly, the *OECD Guidelines* states that

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.\(^{364}\)

The same principles have been provided by the UK data protection law which endorses that

1-Personal data shall be processed fairly and lawfully;
2- Personal data shall be accurate and, where necessary, kept up-to-date.\(^{365}\)

The Malaysian *Personal Data Protection Act 2010*, under the title ‘Data Integrity Principle’, adopts similar requirements with regard to data quality by stating that

---


362 The European Court of Justice states that the ‘right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients.’ *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* [2009] (C-553/07) European Court reports I-03889. at 49.


[a] data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.\(^\text{366}\)

The aim of these requirements such as personal data should be accurate and up to date and the processing of individual’s data shall be done lawfully is to guarantee fairness when data controllers transfer personal information.\(^\text{367}\)

These requirements are significant because they will provide clear procedures for the processing of personal data. Hence, the Libyan legislators should provide similar provisions which would ensure that personal information will be processed under lawful and fair measures because such a policy would ensure integrity.

**Recommendation 4.14:** data protection law should include principle which requires that personal data must be processed fairly and lawfully and shall be accurate and, where necessary, kept up-to-date.

### 4.2.2 The rights of access, rectification and opposition

The aim of data protection law is to provide protection to data subjects. Hence, many data protection laws stipulate some rights that should be given to data subjects in order to reach the outcome that personal data is traded fairly. Data subjects should have the right to access their personal information and correct any mistakes in their information.

With regard to such principles, the EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data states that

\[t\]he data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her.\(^\text{368}\)

---

\(^\text{366}\) Personal Data Protection Act 2010 (Malaysia) s 11.


\(^\text{368}\) EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document Transfers of Personal Data to Third Countries, above n 265, 6.
The EU Directive guarantees to data subjects the power to access personal data that is processed.\textsuperscript{369} Data subjects might order that data to be corrected or deleted and may block data that is incorrect.\textsuperscript{370} If there is no lawful purpose that prevents data subjects from accessing their data or correcting any mistakes, then persons shall constantly have these rights.\textsuperscript{371} It is clear that data subjects should control the way their data is processed and they can stop the processing of their data.

Giving consumers the power over sharing and utilising their personal data is usually considered to influence consumers’ privacy concerns because in such circumstances their confidence will be increased. The value of control is demonstrated by the fact that:

\textsuperscript{369} EU directive 95/46 EC stipulates in Article 12 under title Right of access that:

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

The European Court of Justice held that:

Article 12(a) of the Directive requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.

\textit{College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer [2009] Case (C-553/07) European Court reports I-03889. at 70.}


that consumers show high levels of fears over the use and distribution of personal
data in circumstances where they have no power over their personal data.\footnote{Mary Ann Eastlick et al, ‘Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment’ (2006) 59 Journal of Business Research 879.}

In order to protect personal information, data subjects should have the right to access their personal data and also should have the right rectify such data. Any data protection should ensure these basic rights of data subjects because these principles will contribute to individuals’ confidence in processing their personal information.

**Recommendation 4.15:** data protection law should ensure that data subjects have the right to access, block and correct their personal data.

### 4.2.3 The purpose specification and use or collection limitation principles

This principle requires data controllers to provide notification to data subjects regarding the transfer of their data. This notification will give data subjects all the information that is needed regarding the purpose of processing personal data.\footnote{Jay, above n 367, 231.}

In order to control their data, data subjects should be given notice when data controllers collect, utilise and divulge their private information to third parties. This notice could be done by distributing privacy rules on a web site.\footnote{Robert W Hahn and Anne Layne-Farrar, ‘Benefits and Costs of Online Privacy Legislation’ (2002) 54 (1) Administrative Law Review 91.} For business to access personal information, a reasonable, efficient and lawful manner to obtain such data should be presented.\footnote{A Tasidou, P S Efaimidis and V Katos, Economics of Personal Data Management: Fair Personal Information, Trades Revised Selected Papers submitted to Third International Conference (e-Democracy 2009 Athens, Greece, published in Next Generation Society: Technological and Legal Issues 2010) 151 <http://link.springer.com.ezp01.library.qut.edu.au/chapter/10.1007%2F978-3-642-11631-5_14>, at 20 August 2013.}

Transparency is one of the main objectives of fair information principles because it requires consumers to have knowledge regarding how businesses deal with their data. When data subjects are given notices from data controllers to explain how
personal data is gathered or used, the data subject will be confident and accordingly, such requirement will promote integrity.\footnote{Culnan and Milberg, above n 342, 11.}

The EU Directive supports transparency by ordering data controllers to give notice. The EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data explains that the EU directive 95/46 EC requires that

\[\text{[i]}\text{ndividuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the directive.}\]

**1. The purpose specification principle**

This principle requires that personal information should be processed for a specific purpose or purposes and any further transfer of this information should be linked to the purpose or purposes for which the information was obtained.\footnote{Jay, above n 367, 231.}

The EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data explains that the EU directive 95/46 EC requires that

\[\text{[d]}\text{ata should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.}\]

Furthermore, the OECD, with regard to the collection of personal data, stipulates that

\footnote{Culnan and Milberg, above n 342, 11.}

\footnote{\textquote{Article 11(2) stipulates that when data are collected from someone other than the data subject, information need not be provided to the data subject if this proves impossible, involves a disproportionate effort, or if the recording or disclosure of the data is expressly required by law.' EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Above n 265, 6.}}

\footnote{\textquote{\textquote{Article 13 permits a restriction to the ‘purpose principle’ if such a restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest, or the protection of the data subject or the rights and freedoms of others.’ EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data, above n 265, 6.}}

\footnote{Ibid.}
The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.\footnote{382}

The \textit{Data Protection Act 1998} (UK) stipulates some clear requirements with regard to the purpose specification principle when data controllers obtain personal information:

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.\footnote{383}

The purpose or purposes for which personal data are obtained may in particular be specified

(a) in a notice given for the purposes of paragraph 2 by the data controller to the data subject, or

(b) in a notification given to the Commissioner under Part III of this Act.

In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.\footnote{384}

Data subjects should get clear notice of the purpose(s) for which their personal data is to be processed, in order to not be misled regarding the reason for processing personal data.\footnote{385}

It is important that data protection laws endorse the specific purpose principle because this principle would ensure that data subjects will have enough knowledge regarding the reason for processing their data and also to provide enough safeguards to individuals.


\footnote{383} Data Protection Act 1998 (UK) s 4, sch1.

\footnote{384} Data Protection Act 1998 (UK) s 4, sch1.

2. The use or collection limitation principle

This principle requires that data controllers not only process data for a specific purpose but also the collection and use of personal data shall be limited to the purposes for which personal data is transferred. Consumers ought to have the power to control the way private information is gathered and used, and should also be able to avoid the transfer of personal data to other users if their data is collected for a specific reason but will be used for other circumstances.\textsuperscript{386}

The OECD stipulates such principles by stating that ‘[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means’.\textsuperscript{387}

In addition, the OECD, with regard to the use limitation principle, stipulates that

\begin{quotation}
[p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with paragraph 9\textsuperscript{3}(the Purpose Specification Principle).\textsuperscript{388}
\end{quotation}

This principle provides strong protection to personal information as it enforces limitations on the processing of personal data when data controllers collect and use individuals’ data.

The notice requirement is an imperative right that is given to data subjects to have knowledge regarding the processing of their information. Therefore, data controllers should provide information to data subjects about the reason for collecting data, and the gathering of personal data for different reasons should not be allowed. The application of such principles will increase data subjects’ confidence in the way data is transferred.

\textbf{Recommendation 4.16: privacy law should require data controllers to follow the principles of purpose specification and use or collection limitation in order}

\textsuperscript{386} Culnan and Milberg, above n 342, 11.

\textsuperscript{387} \textit{OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013)} art 7.

\textsuperscript{388} \textit{OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013)} art 10.
to ensure that data subjects are given clear protection regarding the transferring of their personal information.

4.2.4 Consent

The requirement of consent is vital in order to get data subjects involved in the processing of their personal information. Data protection laws require data users to ask for data subjects’ permission to transfer personal data, in particular with processing of data for purposes other than stated. Personal Data Protection Act 2010 (Malaysia) states

[n]o personal data shall, without the consent of the data subject, be disclosed

(a) for any purpose other than

(i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or
(ii) a purpose directly related to the purpose referred to in subparagraph (i). 389

As has been alluded to above, the processing of personal data should be done according to the purpose for which it was collected. However, there are some exceptions to such principles and one of these exceptions is where the individual has provided his or her consent to transfer data for other purposes. 390 As Solove explains ‘[c]onsent performs an enormous amount of work in the law, especially in the law of privacy. It legitimises a wide array of activities and agreements, ones that would be illegitimate and impermissible without consent’. 391

Consent is linked to the process of some major data protection principles such as principles dealing with the collection of sensitive data and utilisation of private data and therefore, consent is not considered as a principle by itself. 392 The provision of

389 Personal Data Protection Act 2010 (Malaysia) s 8.
consent is offering legal obligations that data controllers must fulfil to treat personal data in a specific technique.\textsuperscript{393}

The term ‘consent’ is defined in the Australian \textit{Privacy Act} to mean ‘express consent or implied consent’.\textsuperscript{394} The Macquarie Dictionary defines ‘consent’ as being ‘to give assent; agree; comply or yield’.\textsuperscript{395} The EU \textit{Directive} defines the data subject’s consent ‘as any freely given, definite and informed sign of his desires by which the data subject signifies his agreement to personal data linking to him to be processed’.\textsuperscript{396} The consent is negated if data subjects are not given complete information regarding the conditions of giving consent, or if they are forced to give permission to use their data as a condition to gain benefits.\textsuperscript{397}

The EU \textit{Directive} requires that the data subject should give his or her explicit consent to the processing of personal data. In the online atmosphere, it is really hard for persons to have adequate knowledge about their rights and offer informed permission.\textsuperscript{398} In some circumstances, it is really difficult to understand clearly what may include precise and informed consent to process personal information.\textsuperscript{399}

The \textit{OECD Guidelines}, with regard to the use and collection of personal data, stipulates that

\begin{quote}
[p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law.\textsuperscript{400}
\end{quote}

\begin{footnotesize}
\begin{itemize}
\item[393] Ibid.
\item[394] \textit{Privacy Act 1988} (Cth) s 6 (1).
\item[395] Cited in ALRC Report 108, above n 390, 668.
\item[396] EU Directive 95/46 EC art 2(h).
\item[399] Ibid.
\end{itemize}
\end{footnotesize}
The Personal Data Protection Act 2010 (Malaysia) also requires permission from the data subject to process personal information. However, it provides some exceptions from the requirement of consent. The law stipulates that

1. A data user shall not

   (a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or

   (b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions of section 40.

2. A data user may process personal data about a data subject if the processing is necessary

   (a) for the performance of a contract to which the data subject is a party;

   (b) for the taking of steps at the request of the data subject with a view to entering into a contract;

   (c) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;

   (d) in order to protect the vital interests of the data subject;

   (e) for the administration of justice; or

   (f) for the exercise of any functions conferred on any person by or under any law.

1. Opt-in or opt-out Choice

There are two approaches to gaining permission from a data subject in order to process his or her information. Some may accept the opt-in choice which provides more power to individuals or others might prefer the opt-out choice. This part will discuss and evaluate these two options and try to determine which option might be suitable.

Normally, opt-out options provide that consumers should take some process to defend their private data from collection and data sharing. Opt-in formats provide that data controllers apply some procedures to gain permission from consumers, prior

---

401 Personal Data Protection Act 2010 (Malaysia) s 6 (1-2).
to processing and distributing their information.\textsuperscript{402} Steven Salbu provides comprehensible clarification regarding opt-in and opt-out options:

Specifically, both opt-in and opt-out policies provide a measure of consumer privacy protection, although the former are stronger than the latter. Opt-in policies prohibit businesses from collecting, using, or sharing personal information unless the subject of that information has expressly agreed to these activities. Under an opt-in policy, the default assumption is that every consumer expects privacy. The assumption can be rebutted only through voluntary and affirmative consumer consent. Opt-out policies prohibit businesses from collecting, using, or sharing personal information only after a consumer has taken the initiative to inform the appropriate person or entity of objections to the relevant activities. In contrast to opt-in policies, the default assumption in opt-out policies is that a given consumer does not have privacy expectations regarding relevant activities, such as collecting, using, or sharing the data. To trigger the privacy protections that are automatic under an opt-in policy, a consumer must take the initiative and follow the prescribed steps.\textsuperscript{403}

There are two groups which consider the issue of opt-in and opt-out. On the one hand, business groups support the opt-out choice because this format would permit industry to have access to a huge amount of personal data as there are few options for customers to provide their objections.\textsuperscript{404} The US Competitive Enterprise Institute alleges that the cost of opt-in would be large because consumers may lose the benefits of sharing data

1. The loss of cost-savings that come from using information to control inventory, target marketing, and other types of information-related cost savings. These would be highest for opt-in.
2. The loss of discount pricing offers, savings plans.
3. Losses of time and convenience from, for example, needing to fill out information about oneself repeatedly.\textsuperscript{405}

It is said that many of the US markets are unwilling to apply opt-in standards, so the opt-out choice is the policy adopted by the majority of US firms.\textsuperscript{406} As a consequence, it is suggested that firms might evaluate each system and consider

\textsuperscript{402} Eastlick, above n 372, 879.
\textsuperscript{403} Salbu, above n 235, 661-662.
\textsuperscript{404} Rotenberg, above n 154, [29].
\textsuperscript{406} Eastlick, above n 372, 879.
whether opt-in has benefits above opt-out formats.\textsuperscript{407} However, it is argued that the opt-out system in the US does not reflect the public’s desire, but instead, represents what industry wants.\textsuperscript{408}

On the other hand, supporters of the opt-in choice argue that this choice might reduce customers’ privacy concerns. Furthermore, the time that would be spent by the consumers to opt-out from different firms’ services is another factor that supports the opt-in option.\textsuperscript{409} Jon Leibowitz -the former FTC chairman- suggested that firms should allow customers to choose to opt-in in the circumstances of collecting personal data and more particularly, in the situation of transferring private data with third parties and also if data is shared through different online services.\textsuperscript{410}

The format of opt-out which provides opportunity to consumers to refuse further data sharing might not be efficient.\textsuperscript{411} Especially, it was noticed that there is considerable proof that customers rarely alter the default.\textsuperscript{412} Firms have the motivation to gain benefits from making ‘opting out as cumbersome as possible and do not adequately inform people about the uses of their data’.\textsuperscript{413} Because this is burdensome, few customers opt-out and others who attempt to do so discover that the procedures are difficult to finish.\textsuperscript{414}

In an opt-in system, firms will have the motivation to convince customers to choose opt-in in order to transfer personal data. Such data controllers will find the possible ways to encourage consumers to opt-in.\textsuperscript{415} An opt-in format would support the possibility that instead of choosing according to the default chosen by the business,

\textsuperscript{407} Ibid.
\textsuperscript{408} Rotenberg, above n 154, [29].
\textsuperscript{409} Solove and Hoofnagle, above n 130, 370.
\textsuperscript{411} Solove and Hoofnagle, above n 130, 369.
\textsuperscript{412} Lenard and Paul, above n 4, 6.
\textsuperscript{413} Solove and Hoofnagle, above n 130, 369.
\textsuperscript{414} Ibid.
\textsuperscript{415} Jeff Sovern, ‘Opting in, Opting out, or No Options at All: The Fight for Control of Personal Information’ (1999) 74 \textit{Washington Law Review} 1112.
customers may make their decision depending on their choices.\textsuperscript{416} It is said that ‘[e]vidence on how companies behave in an opt-in environment suggests that such a system may be more efficient for consumers’.\textsuperscript{417} Jeff Sovern states that groups who do not really consider the significance of their data protection privacy are expected to favour an opt-out method, but groups who value their privacy, such as privacy advocates, may prefer an opt-in system.\textsuperscript{418}

Even if the adoption of the opt-in format may increase the cost of services or goods to consumers as well as business, the protection of consumers would be more important than the cost efficiency as consumers with the opt-in format will have full control of their personal data and firms would have the opportunity to ask permission from stakeholders to get access to their private data. However, an opt-out approach to consent would not give consumers strong participation in order to use and collect personal data and instead, firms would have priority over personal information. Jeff Sovern concludes that

> [a]n opt-in system would permit consumers who wish to protect their privacy to do so without incurring transaction costs. Consumers who permit the use of their personal information should also be able to realize their wish easily. Indeed, because firms profit from the use of consumer information, firms would have an incentive to make it as easy as possible for consumers to consent to the use of their personal information.\textsuperscript{419}

With regard to the Libyan context, as has been explained in chapter 2, Sharia law provides strict rules in order to protect the sanctity of private life. The Quran stipulates many restrictive rules in order to provide clear protection to individuals in their privacy. Again, the Quran states

> O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. That is best for you; perhaps you will be reminded. And if you do not find anyone therein, do not enter them until permission has been given you. And if it is said to you, "Go back," then go back; it is purer for you. And Allah is Knowing of what you do.\textsuperscript{420}

\textsuperscript{416} Ibid 1102.
\textsuperscript{417} Ibid.
\textsuperscript{418} Ibid 1101.
\textsuperscript{419} Ibid 1118.
\textsuperscript{420} The Noble Quran (Sahih International Trans) 24: 27-28.
Also, with regard to get permission before accessing private life, the Hadith says that ‘Asking for permission is allowed up to three times. If it is not granted, you must return’. 421

The principle that would be derived from the Quranic and prophetic texts is that prior consent is required before getting access to someone’s private life as the way to protect the sanctity of personal life. Thus, opt-in formats might comply with Sharia law because opt-in options require the permission of individuals to process their personal information before using and collecting personal data.

It appears that the opt-in format complies with the principle of Sharia law as the latter asks permission before getting access to someone’s property. Because the opt-out format would permit businesses to use and collect data and then each individual has the right to prevent further processing, this format may be considered as not complying with Sharia law as there is no prior permission given to access someone’s private life.

Thus, the opt-in option might be preferred over the opt-out format as it would provide more protection for data subjects and encourage business to improve and provide clear procedures of opting-in.

### Recommendation 4.17: data protection law should require data controllers to adopt opt-in formats as it will guarantee extensive protection to personal data.

#### 4.2.5 The security principle

This principle requires data controllers to provide clear security measures in order to protect personal data. To prevent personal data falling into the wrong hands, most data protection laws require data controllers to offer clear processes to secure information from being misused.

To protect information privacy, technical procedures should be in place to defend personal data from unlawful access and also against loss of information. It is said that ‘besides the infringement of privacy as a human right, personal data is at risk of

421 Mukhtasar Sahih Muslim, Hadith 1421.
unauthorised access, falling into the wrong hands, being misused or becoming a commodity for illegal sale’.  

If consumers’ personal data has not been effectively protected, then that may lead to increased identity fraud when consumers are required to provide their identity.  

Security concerns are becoming one of the most important elements for a successful business. Firms may build up systems of recognition that are not built on freely accessible private data and can be simply altered if they are misused by others.

The EU Directive, with regard to securing personal data, requires that

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

Provisions similar to those of the EU which consider the security issue of privacy are provided by the OECD Guidelines and the Malaysian data protection law. The OECD stipulates that

---

423 Ibid.
425 Solove and Hoofnagle, above n 130, 372.
426 EU Directive 95/46 EC art 17.
The Malaysian personal data protection law stipulates that

[a] data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard

(a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

(b) to the place or location where the personal data is stored;

(c) to any security measures incorporated into any equipment in which the personal data is stored;

(d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and

(e) to the measures taken for ensuring the secure transfer of the personal data.  

It is important to require data users to provide strong security procedures to protect individuals from losing control over their personal data. These measures may take different forms such as protecting the place where data is stored, and protecting the transfer of personal data to others and specifically, sensitive information. Data protection laws should consider such principles and provide some technical measures which data controllers should follow.

The Libyan authorities should ensure that any proposed privacy law take into account the security issue. The law should require data controllers to follow reasonable steps to secure information in order to have effective personal data protection. How data is stored and processed should be under clear supervision from the Libyan authorities to achieve the aim of data protection law which is to protect personal data from any damage or harm.

---


428 Personal Data Protection Act 2010 (Malaysia) s 9.
1- Data Security Breach Notification

Some data protection laws adopt the approach that data controllers must give data subjects notices which state that their personal data has been breached. The follow discussion will evaluate the importance of this requirement.

Data breach notification is considered to be a lawful obligation on data controllers in organizations and agencies to inform people that their personal data has been hacked. The outcome of a data breach is that an individual’s security is breached and as a consequence, personal data is revealed without that person’s knowledge.429

It is said that some consumers may not take breach notifications seriously and therefore may disregard notices. However, such ignorance of a breach notification disclosure by some should not prevent offering notices as there are other consumers who would receive these notices and take relevant action.430

Supporters of a data breach notification law provide some reasons to argue the importance of requiring data controllers to notify individuals regarding the breach of their personal information. These reasons include that data breach notification would

1. provide a strong market incentive and stimulus to organizations to secure databases adequately to avoid the brand and reputational damage arising from negative publicity;
2. encourage attention to compliance and vigilance against identity theft; and
3. improve accountability, openness and transparency in the handling of personal information by agencies and organizations.431

The opponents of a data breach notifications’ requirement argue that if breach of personal information is predicted to cause harm to individuals because breached data is considered confidential, then in this situation, data controllers may give notification to data subjects about breach of their data.432 However, if the breach is ‘internal and is quickly remedied so no harm could result, organizations would not

429 Australian Law Reform Commission, above n 284, 1293.
430 Mulligan and Bamberger, above n 424, 3.
431 Australian Law Reform Commission, above n 284, 1306.
necessarily disclose the breach, as disclosure may give rise to unjustified alarm on the part of the individual’. 433

It is interesting to note that the new update of the *OECD Guidelines on Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013) with regard to implement accountability include a provision considering data security breach notification. The *OECD Guidelines* require data controllers to

> provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects. 434

It seems that the reasons provided by the supporters of data breach notification might be stronger than the reasons that support no data breach notification in all circumstances because requiring data users to notify individuals about any breach may encourage data controllers to improve their security systems. Moreover, such notifications would increase transparency of dealing with personal data as people will be confident that there is no misuse of their private or sensitive information.

**Recommendation 4.18:** data protection law should require data controllers to follow reasonable steps to secure data subjects information. Also, the law should adopt data breach notification requirement which requires data controllers to give data subjects notices which state that their personal data has been breached.

### 4.2.6 Enforcement Mechanisms and the Accountability Principle

This principle requires data users to comply with data protection principles and when there is any breach of such rules, data protection law will provide methods to enforce these principles. The *OECD Guidelines* stipulates that ‘[a] data controller should be accountable for complying with measures which give effect to the principles’. 435

---


In the EU there is an agreement that ‘a system of “external supervision” in the form of an independent authority is a necessary feature of a data protection compliance system’.\(^{436}\) Enforcement by government may involve fines which will be enforced by supervision agencies, and further, comprise private law suits brought individually.\(^{437}\)

Enforcement is a crucial aspect of privacy law. This principle will be discussed in more detail in the next chapter which will study the enforcement of data protection law.

### 4.2.7 Restrictions on onward transfers

This principle requires that in order to transfer personal data to different regions, the countries which would receive the personal information should have an adequate data protection system. If these countries do not provide adequate protection to personal data, the processing of personal data should not be accepted.

The EU *Directive* requires an adequate level of protection to take place in any country to which personal data would be transferred.\(^{438}\) As a result, the EU *Directive* generally permits the transfer of personal information only to nations that can provide a sufficient level of data protection.\(^{439}\)

It is stated that ‘Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient is also subject to rules affording an adequate level of protection’.\(^{440}\) Eric Howe claims that

---

\(^{436}\) EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data, above n 265, 6-7.

\(^{437}\) Hahn and Layne-Farrar, above n 374, 91.


\(^{439}\) Ibid 483.

If there is to be a Community with an acceptable and high level of individual data protection, which thereby permits the unrestricted transfer of personal data throughout the Community, then it is to be expected that there will be a fence around the Community with some means of guarding it. Trans-border data flow controls are to be expected and are legitimate.\[^{441}\]

This claim is really strong because if there is no such requirement then the outcome might be like having adequate data protection rules inside the country which restrict the way data is processed, but when the same personal data is transferred to another country where there is no clear data protection the personal data might be under threat. Thus, the adequate data protection requirement in order to transfer data to other countries can guarantee that such an outcome would not happen.

Article 25 of the EU Directive, with regard to restrictions onwards transfers of personal data, stipulates that:

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

A data controller remains accountable for personal data under its control without regard to the location of the data.

A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

\[^{441}\] Eric Howe cited in Schwartz, above n 438, 484.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision. [442]

A number of developing countries have not provided adequate data protection systems which reflect that there are restrictions on the flow of data from the EU. Nevertheless, many EU firms deal with countries that have inadequate privacy systems. [443] This is occurring because of some exceptions stipulated in art 26 of the EU Directive, for example, when data users in the EU can promise that the receiver will obey the data protection policy. [444]

Article 26 of the EU Directive stipulates that

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or


[444] Ibid.
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.445

Malaysia follows a similar approach to the EU Directive in s 129 of the Personal Data Protection Act 2010 under the title ‘Transfer of personal data to places outside Malaysia’. The Act stipulates that

(1) A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette.

(2) For the purposes of subsection (1), the Minister may specify any place outside Malaysia if

(a) there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or

(b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act.446

445 EU directive 95/46/EC, art 26.

446 Personal Data Protection Act 2010 (Malaysia) s 129 1-2.
The Malaysian law also provides some exceptions on the restriction of transfer of personal data outside Malaysia where that place does not have an adequate level of data protection.\footnote{\textit{Personal Data Protection Act 2010} (Malaysia) s 129 (3) stipulates that: Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if}

It seems that the restriction of processing personal data to an outside country by requiring an adequate data protection in that country is a valuable requirement because the aim of data protection law is to provide a strong defence to processing personal information, whether this data is being processed inside the nation or outside.

Personal data should be under clear protection and should be treated according to the principles of data protection. Hence, when personal data is sufficiently protected by the data protection law if it is processed inside the country and not sufficiently protected if processed outside the nation, that result may clash with the aim of data protection law.

\footnote{\textit{Personal Data Protection Act 2010} (Malaysia) s 129 (3) stipulates that: Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if}

(a) the data subject has given his consent to the transfer;

(b) the transfer is necessary for the performance of a contract between the data subject and the data user;

(c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which

(i) is entered into at the request of the data subject; or

(ii) is in the interests of the data subject;

(d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;

(e) the data user has reasonable grounds for believing that in all circumstances of the case—

(i) the transfer is for the avoidance or mitigation of adverse action against the data subject;

(ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and

(iii) if it was practicable to obtain such consent, the data subject would have given his consent;

(f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act;

(g) the transfer is necessary in order to protect the vital interests of the data subject; or

(h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister.
The adequacy principle may strengthen the application of data protection law because many countries would improve their privacy standards in order to meet the adequacy requirement of the processing country. Therefore, it is believed that this principle should be included in the Libyan privacy framework.

**Recommendation 4.19:** data protection law should commonly permit the transfer of personal information only to nations that can provide a sufficient level of data protection.

### 4.3 Conclusion

This chapter considered some main elements of data protection law, from the scope of data protection law to the basic principles of data protection. The first section of this chapter examined the scope of data protection law and found it has been done by providing the general directions that are usually adopted by most data protection laws. In order to get a clear image regarding the application of data protection law, some related terms have been defined and clarified. Finally, some exceptions from the law’s implementation have been evaluated and it has been determined whether they should be adopted or not.

The chapter argued that in order to have a strong privacy law, a wide scope of legislation should be the choice. Fewer exceptions on data protection law should be the direction of Libyan policy-makers as that will add more credibility to any privacy Act. Once privacy law allows many exemptions to its application, that might lead to reduce the integrity of any privacy legislation.

The second section provided the basic principles of data protection law, by providing the approach of the EU Directive95/46 EC on the Protection of Personal Data and the *OECD Guidelines* (2013).

The Libyan legislature should take into account the issues that have been raised in this chapter in order to determine which approach is suitable for the Libyan context and accordingly, form legislation that benefits from the practice of other legal systems. The law should identify vital areas of privacy concerns and stipulate the basic principles for dealing with personal data.
Chapter V

Enforcement of privacy law

It is not sufficient to introduce new legislation to organise or control specific areas of conflict or debate; it is also necessary that the new legislation provides appropriate mechanisms to apply the laws successfully. If there are no procedures regarding the enforcement of the law, it might reflect negatively on the effectiveness of the law. Privacy law is mainly enforced to protect personal data in the circumstances where such personal data is under attack by others. Any privacy legislation, in order to be implemented effectively, needs a strong authority that takes into consideration the enforcement of such law. Therefore, most data protection laws include provisions regarding the enforcement of the law such as establishing a Data Protection Commission, providing remedies and imposing sanctions.

This chapter will discuss the appropriate ways to enforce privacy law to ensure that Libya will have adequate protection of personal data. In particular, it will investigate the need to create a Data Protection Commission, and what functions and powers should be given to the Commission, and the requirements that a Data Protection Commission should meet in order to have a successful supervisory authority. In order to achieve that, international attempts which have considered the creation of supervisory agencies will be examined and also, when appropriate, some legislation that introduced a Data Protection Authority will be evaluated such as the Malaysian and Moroccan laws.

Furthermore, the second part of the chapter will analyse two aspects of forcing data controllers to respect data subjects’ rights. These aspects are promoting remedies and imposing sanctions when there is any contravention of privacy law.

---


449 Ibid.

5.1 Data Protection Commission

Many data protection laws create Data Protection Authorities (DPAs). Most countries that adopted data protection laws have established a Data Protection Commission in order to supervise the application of the law. A Data Protection Authority, as defined by the EU Directive, is ‘one or more public authorities [which] are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive’. Flaherty argues that ‘[i]t is not enough simply to pass a data protection law in order to control surveillance; an agency charged with implementation is essential to make the law work in practice’. These supervisory authorities are separate agencies whose main mission is to oversee the implementation of the privacy laws, even though those agencies worldwide might be varied with regard to their agendas, powers, priorities, and assets. Data Protection Authorities aim to oversee the processing of personal data by private

---

451 ‘Privacy Enforcement Authority means any public body, as determined by each Member country, that is responsible for enforcing Laws Protecting Privacy, and that has powers to conduct investigations or pursue enforcement proceedings.’ OECD, Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy (2007) 8 <http://www.oecd.org/sti/ieconomy/38770483.pdf> at 20 August 2013.

452 The OECD Report on the Cross-Border Enforcement of Privacy Laws (2006) states that [n]early all OECD members have data protection laws – most of which follow the principles of the Privacy Guidelines – and have established authorities to carry out enforcement responsibilities. If member country authorities share commonalities in terms of the powers they have and the scope of the laws they enforce, certain variations remain. Some authorities are charged with resolving individual complaints, others with supervising regulatory compliance, and many do both. Variations exist with respect to complaint handling processes, the authority to investigate or audit, and the available sanctions and remedies for a breach. Some are independent authorities, some housed within government departments. Some cover the public sphere, others only the private sector, and many cover both. A few authorities are mandated to enforce privacy laws covering a particular field.


453 EU Directive 95 s 28.


455 EU Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, above n 450, 4.
sectors such as firms or organisations, as well as the processing of personal data by public sectors like government institutions.456

The need for a supervisory authority to consider the protection of personal information has gained global recognition.457 An increasing number of these institutions worldwide may give an indication that these supervisory agencies are valuable for effective data protection.

Data Protection Authorities explore any matters related to the law that is not clear enough and this is done by providing advice, opinions and explanations and also by conducting investigations.458 In some regimes, Data Protection Commissions are also responsible for the enforcement of privacy law by enforcement notices and civil penalties.459 These powers reflect the value of introducing such an agency in any country that establishes privacy law.

Jay Stanley demonstrates the value of introducing data protection commission in the US. Stanley argues that

[t]he United States urgently needs stronger privacy oversight institutions to serve as a countervailing force as the computer and telecommunications revolutions change the privacy landscape for Americans and create new opportunities for large institutions to grab more power at the expense of ordinary people. Only by creating such institutions can we ensure that American values are preserved and the rights and interests of ordinary people are protected.460

Graham Greenleaf argues that the Asia-Pacific nations, whose privacy laws adopt an independent Data Protection Commission, present a stronger protection of personal data than nations whose laws do not present such a supervisory authority.461

---


458 Ibid 1186.

459 See Data Protection Act 1998 (UK) ss 40, 55.

460 Stanley, above n 448, 4.

It is clear that there is strong support for introducing supervisory authorities to oversee the implementation of privacy law. There are many international and regional attempts which recognise the importance of establishing supervisory authorities, some of which are as follows:

1- In 1990, the UN General Assembly introduced Guidelines for the Regulation of Computerized Personal Data Files. These Guidelines considered principles concerning the minimum guarantees that should be provided in national legislation. With regard to the enforcement principle, the resolution stipulated that

\[
\text{[t]he law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles.}^{462}
\]

2- Because the protection of personal information is a human rights matter, it is suggested that the UN Resolution which considers national institutions for the promotion and protection of human rights are evidently applicable to supervisory privacy agencies.\(^{463}\) The UN Resolution

- \([r]eaffirm[s] \) the importance of developing, in accordance with national legislation, effective national institutions for the promotion and protection of human rights.
- \([e]ncourage[s] \) Member States to establish or, where they already exist, to strengthen national institutions for the promotion and protection of human rights and to incorporate those elements in national development plans.\(^{464}\)

These principles which were adopted by the United Nations in 1993 obviously indicate the value of and the need to introduce national institutions for protecting human rights and privacy is one of those matters that are directly linked to human rights issues.

3- The EU Directive requires each EU member to create a supervisory authority by stipulating that

\(^{462}\) Guidelines for the Regulation of Computerized Personal Data Files, UN doc 45/95 (14 December 1990). 8.


[e]ach Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.\(^{465}\)

4- The Council of Europe’s Convention 108 Additional Protocol (2001) whose purpose is to develop the role of the principles that are included in the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No108, “the Convention”)\(^{466}\) by adding new provisions.\(^{467}\) The Additional Protocol requires the establishment of data protection agencies by stipulating that

[ e]ach Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.\(^{468}\)

5- The Madrid international Conference of Data Protection Agencies adopted, in 2009,\(^{469}\) a ‘Joint Proposal for a draft of International Standards on the Protection of Privacy with regard to the Processing of Personal Data’ requiring that

in every State there shall be one or more supervisory authorities, in accordance with its domestic law, that will be responsible for supervising the observance of the principles set out in this Document.\(^{470}\)

\(^{465}\) EU Directive 95/46 EC art 28 (1).

\(^{466}\) The Member States of the Council of Europe consider that the aim of the Council of Europe ‘is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms. [Also, it provides] that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing’. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108, opened for signature 28 January 1981, (entered into force 1 October 1985).


\(^{469}\) The Madrid Conference is ‘the joint efforts of the privacy guarantors from fifty countries, coordinated by the Spanish Data Protection Agency, [and] has resulled in a text that seeks to reflect the many approaches that the protection of this right allows for, by integrating legislations on five continents’. Artemi Lombarte, International Standards on the Protection of Privacy with regard to the Processing of Personal Data, The Madrid Resolution (2009) < http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf> at 9 July 2013.
It is noticeable that there is international recognition of the value of creating Data Protection Commission in any countries that need to protect the individual right to personal data adequately. The South African Law Reform Commission explained the aim of Data Protection Authorities in the follow three points:

- To deliver a satisfactory level of compliance with the rules contained in the information protection legislation;
- to provide support and help to data subjects in the exercise of their rights;
- to provide appropriate redress to prejudiced data subjects where rules are not complied with.471

Furthermore, a data protection commission can play a significant role in uniting the views regarding privacy matters worldwide. The OECD recommendation of the council on cross-border co-operation in the enforcement of laws protecting privacy recognised that

while there are differences in their laws and enforcement mechanisms, Member countries share an interest in fostering closer international co-operation among their privacy law enforcement authorities as a means of better safeguarding personal data and minimising disruptions to transborder data flows.472

Supervisory authorities play a significant role in terms of implementing privacy law and the majority of data protection laws introduce such an agency in their legislation. Therefore, the next sections will study these authorities by evaluating the power and functions that they should be given and also the requirements that they should meet in order to have an effective supervisory authority.

5.1.1 The power of a Data Protection Commission

In order to carry out their work, supervisory authorities should be given a legal capacity to perform their duties. Many data protection laws indicate that every State


should endorse some powers for the commissioners. The EU Directive provides some powers to supervisory authorities so they can perform effectively including:

A- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;

B- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;

C- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.473

In the same way, the OECD calls upon member countries to adopt some procedures to guarantee that Data Protection Authorities have adequate powers to stop any infringements of privacy laws.474

The Australian Privacy Act 1988 (Cth) states that ‘the commissioner has power to do all things that are necessary or convenient to be done for, or in connection with, the performance of his or her functions’.475 Similarly, the Moroccan Personal Data Protection Act 2009 gives the commissioners of the Data Protection Authority powers of monitoring and authorising the processing of personal data.476

Libyan policy-makers should provide enough powers to the supervisory agency in order that the commissioners can conduct their work effectively. It is important that privacy authorities in Libya be given powers such as having access to personal data for investigative purposes because without these powers, any Data Protection

475 Privacy Act 1988 (Cth) s 27 (2).
Authority might suffer from some weaknesses in practice. The powers that are endorsed by the EU Directive might be used as a guide for the Libyan authorities.

**Recommendation 5.1: privacy law should give Data Protection Authority adequate powers in order to perform effectively.**

### 5.1.2 The functions of a Data Protection Commission

Data Protection Authorities offer a practical approach to reducing stakeholders’ fears regarding their privacy, as well as minimising costly litigation because supervisory authorities usually have the opportunity to quickly reply to privacy complaints.\(^{477}\) In some cases the DPA has the ability to impose civil penalty directly; in other circumstances, the findings by the DPA are preliminary only and can lead to negotiated settlements or further court action to enforce the law.

It is recommended that a Data Protection Authority should not only be an advisory committee but also should have supervisory rights which are affiliated with legal powers.\(^{478}\) Data Protection Authorities should have the power to play important roles in fields such as ‘compliance, supervision, investigation, redress, guidance and public education’.\(^{479}\) It is suggested that Data Protection Authorities are not only ‘expected to serve as ombudsmen, auditors, consultants, educators, policy advisers and negotiators, but they should also be able to enforce changes in behaviour, when private or public actors violate data protection legislation’.\(^{480}\) Colin Bennett demonstrates that the commissioner of data protection is ‘an ombudsman for citizen complaints, an auditor of organizational practices, a consultant on new and existing

\(^{477}\) Rotenberg, above n 154, [95].


\(^{479}\) Ibid.

information systems, an educator of the public, a policy adviser, and a quasi-judge’. 481

The next discussion will provide some of the functions of a data protection commission which have been derived from the practice of different privacy laws.

A- Investigating contraventions of the law

One of the aims of data protection commissioners is to implement the law in order to guarantee the adequate protection of personal information. Personal Data Protection Act 2010 (Malaysia) stipulates that the commissioners aim to

implement and enforce the personal data protection laws, including the formulation of operational policies and procedures. 482

In order to enforce the law, data protection authorities must have the right to investigate any disagreement involving privacy principles. The majority of data protection laws provide such provisions. In the circumstances where problems linked to privacy matters exist, supervisory authorities ought to carry out a suitable examination and decide what occurred and how the issues should resolved. 483

The EU Directive provides that

[ e]ach supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim. 484

Similarly, the Malaysian law gives the commissioners the power to hear and investigate claims. The commissioners

monitor and supervise compliance with the provisions of this Act, including the issuance of circulars, enforcement notices or any other instruments to any person. 485

482 Personal Data Protection Act 2010 (Malaysia) s 48(b).
483 Stanley, above n 448, 7.
484 EU Directive 95/46 EC art 28 (4), supervisory authority.
485 Personal Data Protection Act 2010(Malaysia), s 48(g).
According to Moroccan law, the data protection commission ‘may conduct investigation and inquiries, as well as collect all the documents necessary for its mission’.

In addition, the Australian Privacy Act 1988 gives the commissioners the right to investigate any breach of privacy law. The law requires commissioners to investigate an act or practice of an agency that may breach an Information Privacy Principle and, where the Commissioner considers it appropriate to do so, to endeavour, by conciliation, to effect a settlement of the matters that gave rise to the investigation.

The Canadian Personal Information Protection and Electronic Documents Act 2000 also offers to the commissioner the power to investigate any breach of the law when an individual complain about such matters. The law provides that

1. An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1.

2. If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter.

It seems that most data protection laws offer to the commissioners the power to investigate and hear any complaints when there is a contravention of the privacy principles. Libyan policy-makers should provide this function to data protection commission in order to guarantee that individuals find an easy and cheap process of complaint in the circumstances where their data is under threat. The commissioners should be able to investigate any breach of privacy law.

Recommendation 5.2: Data Protection Authority should be given the power to hear claims concerning the protection of personal data and also investigate any breach of privacy law.

486 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (t-pd), above n 476, 6-7.

487 Privacy Act 1988 (Cth) s 27(1) (a).

488 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 11.
B- Publishing the activities of commissioners

Many data protection laws stipulate that Data Protection Authorities should publish reports regarding the activities conducted by the commissioner. These reports would guarantee transparency, integrity and would also lead the public to trust in the commissioners’ performance.

The EU Directive requires privacy authorities to report their activities:

   each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.  

Also the Canadian Personal Information Protection and Electronic Documents Act 2000 provides that

   the Commissioner shall, as soon as practicable after the end of each calendar year, submit to Parliament a report concerning the application of this Part, the extent to which the provinces have enacted legislation that is substantially similar to this Part and the application of any such legislation.

It is believed that data protection commissioners should publish their reports concerning the application of law because these reports would provide a level of confidence between individuals and commissioners as the commissioners’ activities will be available to the public.

**Recommendation 5.3: Data Protection Authorities should be required to publish reports regarding the activities conducted by the commissioner.**

C- Providing Advice with regard to implementing the law

Some data protection laws require the supervisory agency to provide advice to the minister or any organisations regarding any matters linked to protecting personal information. ‘With the privacy and technology landscape constantly in a state of rapid change, a privacy officer is needed not just to perform specific bureaucratic

---


490 Personal Information Protection and Electronic Documents Act, SC 2000 c5 (Canada) s 25(1).
functions but also to provide broad public leadership and guidance on how to protect privacy and other liberties'. The EU Directive requires that each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals’ rights and freedoms with regard to the processing of personal data.

The Australian Privacy Act (1988) requires the commissioners to provide advice to a minister, agency or organisation on any matter relevant to the operation of the Act.

Furthermore, Australian privacy law gives the commissioner the power to make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of the privacy of individuals.

Similarly, the Malaysian law provides the same function by requiring the commissioners to advise the Minister on the national policy for personal data protection and all other related matters.

This opportunity to advise the minister or organisation about any legal matters is significant because when there is any misunderstanding regarding any privacy matters, the commissioners may advise the minister or organisation with regard to the appropriate meaning. The commissioners have the ability to effectively achieve this aim as the commissioners are among the most qualified in the area of privacy concerns because they deal with the issues of privacy principles daily.

**Recommendation 5.4: Data Protection Authority should have the right to provide Advice with regard to implementing the privacy law.**

---

491 Stanley, above n 448, 8.
492 EU Directive 95/46 EC art 28(2).
493 Privacy Act 1988 (Cth) (Australia) s 27 (1)(f).
494 Privacy Act 1988 (Cth) (Australia) s 27 (1)(r).
495 Personal Data Protection Act 2010 (Malaysia), s 48 (a).
496 See Bennett, above n 481, 225.
D- Determining whether outside country has adequate protection of personal data

Data protection laws provide some restrictions on transferring data outside the country. This restriction requires that the countries which will receive the personal data have adequate protection of personal information. Some data protection laws give the Data Protection Commission the authority to determine whether the place outside the country provides effective personal data protection. The Malaysian law takes this direction by giving the commissioners the right to determine, in pursuance of section 129, whether any place outside Malaysia has in place a system for the protection of personal data that is substantially similar to that as provided for under this Act or that serves the same purposes as this Act.497

Similarly, the Moroccan law gives the national commission the right to prepare a list of countries that have adequate protection of personal data.498

Libyan policy-makers should provide this function to data protection commissioners because those commissioners are closely connected to the issue of personal data and it would be easier for them to determine whether outside countries have sufficient protection for personal information or not.

**Recommendation 5.5: data protection law should give a Data Protection Commission the power to decide whether the place outside the country provides efficient personal data protection.**

E- Conducting research

Many data protection laws require Data Protection Authorities to conduct research regarding the emerging issues of personal protection and the effectiveness of new technology on the protection of personal data and to recommend any necessary amendments to privacy law. The *Personal Data Protection Act 2010 (Malaysia)* requires the commissioners to undertake or cause to be undertaken research into and monitor developments in the processing of personal data, including technology, in order to take account

497 *Personal Data Protection Act 2010 (Malaysia)*, s 48 (e).
498 *Personal Data Protection Act 2009 (Morocco)*, s 43.
any effects such developments may have on the privacy of individuals in relation to their personal data.\footnote{499}{The Malaysian Personal Data Protection Act 2010(Malaysia), s 48 (f).}

In the same way, The \textit{Australian Privacy Act 1988}(Cth) requires the commissioner to undertake research into, and to monitor developments in, data processing and computer technology (including data-matching and data-linkage) to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results of such research and monitoring.\footnote{500}{Privacy Act 1988 (Cth) s 27 l (c).}

The Canadian \textit{Personal Information Protection and Electronic Documents Act} 2000 provides similar provisions requiring the commission to conduct research regarding any related matters. The law requires the commissioner to undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry.\footnote{501}{Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (Canada) s 24 (b)}

It is believed that the Data Protection Commission should play an important role with regard to examining new issues related to privacy and recommend any amendments that are needed to keep personal information in a safe place. Therefore, the Libyan authorities should ensure that the commissioners have the right to conduct research and recommend amendments to the law.

\begin{boxed}{Recommendation 5.6: the commissioners of Data Protection Authority should have the power to carry out research and recommend amendments to the law.}

\begin{section}{F- Initiating educational programs}

Data Protection Authorities should play a significant role in educating individuals about their rights and the process of defending their rights. Thus, some privacy laws require data protection commissioners to commence educational programmes in order to promote the privacy of individuals. The Australian law requires the commissioners to undertake educational programs on the Commissioner’s own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner.\footnote{502}{Privacy Act 1988 \textit{(Cth)} s 27 1 (c).} 

\begin{flushright}
\textit{The Malaysian Personal Data Protection Act 2010(Malaysia), s 48 (f).}
\end{flushright}

\begin{flushright}
\textit{Privacy Act 1988 (Cth) s 27 l (c).}
\end{flushright}

\begin{flushright}
\textit{Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (Canada) s 24 (b)}
\end{flushright}

142
Similarly, the Malaysian law stipulates that the commissioners are required to promote awareness and dissemination of information to the public about the operation of this Act.\textsuperscript{503}

The Canadian \textit{Personal Information Protection and Electronic Documents Act} has a similar provision requiring the commission to develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part.\textsuperscript{504}

This is one of the vital roles of the commissioners because educating individuals about their rights will lead those individuals to know about the processes and the procedures necessary to prevent their personal information from being misused and falling prey to deceptive conduct and to take legal action when their personal information is at risk.

\begin{center}
\textbf{Recommendation 5.7: data protection law should require the commissioners of Data Protection Authority to develop and conduct information programs to foster public understanding of the law.}
\end{center}

These functions of Data Protection Commission indicate the value of these supervisory authorities in countries. There is clear support for such agencies because these authorities enforce privacy principles and ensure that data controllers are following the privacy standards.

The next section will examine the requirements of establishing an effective Data Protection Commission.

\textbf{5.1.3 Establishing an effective Data Protection Commission}

This section will examine the requirements for establishing a strong data protection authority and then will evaluate the practice of Malaysia and Morocco with regard to their Data Protection Authority. Finally, the creation of the Libyan Data Protection Commission will be examined.

\textsuperscript{502} \textit{Privacy Act 1988 (Cth)} s 27 1(m).
\textsuperscript{503} \textit{Personal Data Protection Act 2010} (Malaysia) s 48 (h).
\textsuperscript{504} \textit{Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)} (Canada ) s 24 (a).
5.1.3.1 The requirements for establishing an effective Data Protection Commission

The importance of creating Data Protection Authorities in a country in order to enforce data protection law was discussed earlier. The supervisory agency plays a vital role in implementing privacy law but to achieve its aim, this agency should be established by following specific requirements.

Alex Turk, the former president of the French National Commission of Information and Liberties (CNIL), stressed that to have an effective data protection authority, the agency should meet the requirement of autonomy and integrity. Turk demonstrated that the aim of Data Protection Authorities should be to respond to the various issues that are linked to the security of individuals’ data.

A. Independence

This is the most significant condition required for successful Data Protection Authorities because if the commissioners are independent of any external authorities such as government’s agencies in performing their work, the commissioners will carry out their job effectively without any fear.

It is suggested that the two main threats to independence are the ability of governments to organize the budget of a Data Protection Authority, and the government’s ability to choose commissioners. The European Union Agency for Fundamental Rights states that ‘the guarantee of independence is, in fact, primarily assured by the procedure of nomination and removal of the officers of the DPAs. The control over financial resources represents a second relevant element in ensuring the autonomy of supervisory authorities’.

---

506 Ibid.
507 Flaherty, cited in Greenleaf, above n 454, 4.
The *EU Directive* requires that the privacy authorities, in order to practice their roles in enforcing privacy principles, should be fully independent.\(^509\) It is said that ‘it seems tremendously important, not only to strengthen DPAs’ independence, particularly from public policy-makers, but also to increase their financial and personnel resources significantly in order to enhance their effectiveness’.\(^510\)

Data Protection Authorities should have enough resources to use their powers and functions because without suitable resources, the agency will not be able to perform effectively.\(^511\) It is argued that ‘some privacy officials complained that they simply didn’t have sufficient resources to do anything but react to complaints, not to mention carrying out the full extent of their powers under the law’.\(^512\) With regard to the value of creating an independent data protection authority, it is demonstrated that DPAs are particularly under threat of being held in check by public authorities. Since the State not only delegates power to DPAs, but could additionally be subject to harsh criticism and potentially strict regulations itself, public actors have an increased interest in manipulating the output and outcome of DPAs’ actions.\(^513\)

Only an independent organisation is capable of criticizing the performance of the executive branch.\(^514\) It is obvious that when data commissioners are supervised by government agencies, the commissioners will find it hard to criticise and evaluate the government’s respect of privacy because if government activities with regard to privacy matters were criticised, the governments may find ways to prevent data commissioners from doing their job effectively.

Lee Bygrave states that creating an independent Data Protection Authority will lead the authority to build its judgment only on the subject matter of the case, without involvement by other entities which may force the authority to adopt particular

---

\(^509\) *EU Directive* 95/46 EC, art 28 (1).

\(^510\) Schütz, above n 456, 141.

\(^511\) Stanley, above n 448, 9.

\(^512\) Ibid.

\(^513\) Schütz, above n 480, 50.

\(^514\) Gellman, above n 457, 1208.
decisions. Geoffrey Miller, with regard to the value of independent authorities, states that

[i]ndependent agencies are relatively insulated from political pressures. This insulation, it is said, will encourage decisions on the substantive merits of the case, thus enhancing the beneficial effects of agency expertise. More broadly, insulation from political pressures is calculated to reduce the influence of factions or interest groups and thereby to serve the broad ideals that inspired the Framers of the Constitution.

Miller shows the significance of having an agency independent of government interference in the US, by stating that there is a need for an independent agency because such an independent authority makes its judgments depending on the substantive elements of the case, without considering other factors. Not requiring that data protection commissioners be independent might lead the agencies to make their judgments in favour of interest groups.

There are many international and regional attempts such as resolutions, directives and conferences which recognise the significance of establishing independent privacy agencies:

1- In 1990, the UN General Assembly introduced Guidelines for the Regulation of Computerized Personal Data Files. These Guidelines considered principles concerning the minimum guarantees that should be provided in national legislation. With regard to the enforcement principle, the resolution stipulated that

[t]his authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence.

2- The UN Resolution (1993), which considers national institutions for the promotion and protection of human rights, considers the need for independent

---

517 Guidelines for the Regulation of Computerized Personal Data Files, UN doc 45/95 (14 December 1990) 8.
authorities in order that these institutions will work effectively. The UN decree stipulates that

- the national institution shall have an infrastructure which is suited to the smooth conduct of its activities, in particular adequate funding. The purpose of this funding should be to enable it to have its own staff and premises, in order to be independent of the Government and not be subject to financial control which might affect its independence.

- in order to ensure a stable mandate for the members of the national institution, without which there can be no real independence, their appointment shall be effected by an official act which shall establish the specific duration of the mandate. This mandate may be renewable, provided that the pluralism of the institution’s membership is ensured.518

3- Similarly, the Council of Europe Convention 108 Additional Protocol (2001) also endorses the importance of having an independent body by providing that ‘the supervisory authorities shall exercise their functions in complete independence’.519

4- During the 23rd International Conference of Data Protection Commissioners (Paris, 2001), accreditation features of data protection authorities were suggested. With regard to autonomy and independence, it was concluded that a Data Protection Commission has to have its sovereignty and independence in order to successfully supervise the application of privacy principles.520 The conference further explained the requirement of autonomy by arguing that

[a]utonomy requires that an authority be empowered, both in a legal and practical fashion, to initiate and undertake appropriate action without having to seek others’ permission. Independence is important for agencies to be able to operate free from political or governmental interference and to withstand the influence of vested interests. Typical guarantees include:

1- Appointment for a fixed term;

2- Removal only for inability to perform the office, neglect of duty, or serious misconduct;

---


519 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, CETS No 181 opened for signature 8 November 2001, Strasbourg (entered into force 1 July 2004) art 1 (3).

3- The power to report directly to the head of government or legislature and to speak publicly on matters of concern;

4- Immunity against personal lawsuit for actions carried out as part of official duties;

5- Power to initiate investigations.\textsuperscript{521}

5- Furthermore, the Madrid International Conference of Data Protection Authorities adopted, in 2009,\textsuperscript{522} a ‘Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the Processing of Personal Data’ requiring that the supervisory authorities

shall be impartial and independent, and will have technical competence, sufficient powers and adequate resources to deal with the claims filed by the data subjects, and to conduct investigations and interventions where necessary to ensure compliance with the applicable national legislation on the protection of privacy with regard to the processing of personal data.\textsuperscript{523}

The Madrid Declaration calls on every country to introduce a supervisory authority and requires these privacy authorities to be independent in order to perform their work effectively.

These international attempts from resolutions to conferences try to ensure the importance of having an independent Data Protection Authority in the country. In this context, it is vital to provide the decision of the European Court of Justice in the case between the European Commission and the Federal Republic of Germany. The court stated that

The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It

\textsuperscript{521} Ibid.


was established, not to grant a special status to those authorities themselves and their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions. It follows that, when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State.\footnote{European Commission v Federal Republic of Germany [2010] (C-518/07) European Court Reports I-01885 at 25.}

It is clear that the court recognised the significance of introducing an independent Data Protection Commission because an independent agency will perform effectively and accordingly, will make decisions depending on the circumstances of each case.\footnote{In the case between European Commission v Republic of Austria, the European Court of Justice (ECJ) held that the Austrian Data Protection Authority (DPA) Datenschutzkommission (DSK) does not meet the requirements of independence within the meaning of the second subparagraph of Article 28(1) of the European Data Protection Directive (95/46/EC). The Court declares that by failing to take all of the measures necessary to ensure that the legislation in force in Austria meets the requirement of independence with regard to the Datenschutzkommission (Data Protection Commission), more specifically by laying down a regulatory framework under which - the managing member of the Datenschutzkommission is a federal official subject to supervision, - the office of the Datenschutzkommission is integrated with the departments of the Federal Chancellery, and - the Federal Chancellor has an unconditional right to information covering all aspects of the work of the Datenschutzkommission, The Republic of Austria has failed to fulfil its obligations under the second subparagraph of Article 28(1) of Directive 95/46/EC of the European Parliament. \footnote{European Commission v Republic of Austria [2012] (C-614/10) European Court Reports.}\footnote{Data Protection Act 1998(UK) sch 5 - 1(2).}}

Any Data Protection Authority has to be free from any interference from the government. In order to ensure the independence of the UK Information Commission, the UK data protection law stipulates that the commissioners are not servants or agents of the Crown.\footnote{Data Protection Act 1998(UK) sch 5 - 1(2).}

\textbf{B. Transparency}

The second essential element of creating an effective Data Protection Commission is that the supervisory agency shall reflect transparency in practising its power. Graham
Greenleaf and others, with regard to privacy authorities’ transparency, demonstrates that

[m]ost of the Commissioner’s improvements in transparency have come from making public submissions to Parliamentary or other enquiries where public submissions are invited, or sometimes where the Commissioner is specifically invited to submit.\[527\]

An earlier section of this thesis considered the commissioners’ function in implementing data protection law and how the commissioners are required to publish a report with regard to their activities. The purpose of providing a regular report regarding the performance of the commissioners is to encourage integrity. Greenleaf suggests that the requirement to publish the commissioners’ activities has promoted the principle of transparency. It is said that transparency should be acquired through the performance of the commissioners and this integrity can be achieved by offering annual reports to Congress and accordingly, to the community.\[528\] The Data Protection Commission should distribute its reports with regard to the issue of processing personal data and these reports should be provided to the public.

It is clear that the requirement of transparency would enhance the work of the commissioners and accordingly, the public would trust in such an authority because there would be nothing to hide. Therefore, there are many procedures through which commissioners would ensure integrity in their work such as publishing their documents regarding their funds, decisions and choices.

To sum up, with regards to the requirements that Data Protection Authorities should meet in order to work effectively, it is suggested that

[t]rue independence is a multi-faceted concept that goes beyond requiring the DPA to have a particular legal structure. Rather, an evaluation of a number of elements is required, such as being insulated from political influence; having a sufficient budget to do its job properly; and being able to hire sufficient numbers of qualified staff, while at the same time being able to ensure sufficient accountability. Fulfilling all these factors simultaneously is a tall order, but will


\[528\] Abu Bakar Munir, cited in Habib, above n 324.
become increasingly necessary to ensure the legitimacy and credibility of data protection supervision and enforcement in the years ahead.\textsuperscript{529}

This statement summarises the requirements that the supervisory agency should meet in order to guarantee its authenticity and reliability. It is said that it is not easy to meet all the requirements but these requirements are important for effective data protection commissioners. Thus, it is believed that the Libyan policy-makers should provide enough legal grounds to make sure that any proposed privacy agency will meet such important basics.

**Recommendation 5.8: data protection law should ensure that data protection authority meet the requirement of autonomy and transparency.**

The next discussion will provide the experience of two different jurisdictions which have similar backgrounds to Libya, the practices of Malaysia and Morocco. It will examine whether the Data Protection Commission in those two countries have met the requirement of having an independent authority.

5.1.3.2 The Malaysian and Moroccan experience

It is important to study how the Data Protection Authority is created in Malaysia and Morocco because it is valuable to recognise the limitations that such authorities face in those countries. Libya could learn from their experience when policy-makers attempt to establish a supervisory authority in Libya.

A. The Malaysian Data Protection Commission

The Malaysian *Personal Data Protection Act 2010* introduces Data Protection Commission and the law stipulates the process of establishing such an authority. The Malaysian Act, under the title ‘Appointment of Commissioner’, gives the minister, who is charged with the responsibility for the protection of personal data,\textsuperscript{530} the power to choose any person to be the Personal Data Protection Commissioner. The law stipulates that

\begin{itemize}
\item[530] *Personal Data Protection Act 2010* (Malaysia), s 4.
\end{itemize}
(1) The Minister shall appoint any person as the “Personal Data Protection Commissioner” for the purposes of carrying out the functions and powers assigned to the Commissioner under this Act on such terms and conditions as he thinks desirable.

(2) The appointment of the Commissioner shall be published in the Gazette.\textsuperscript{531}

It is apparent that the Minister plays a significant role in appointing the Personal Data Protection Commissioner. The lack of independence of the privacy authority is considered one of the most noteworthy limitations of the Malaysian law which can be noted in art 59\textsuperscript{532}. Article 59 provides that:

(1) The Commissioner shall be responsible to the Minister.

(2) The Minister may give to the Commissioner directions of a general character consistent with the provisions of this Act relating to the performance of the functions and powers of the Commissioner and the Commissioner shall give effect to such directions.\textsuperscript{533}

Because the commissioners are responsible to the minister, the independence of commissioners who monitor the processing of personal data in a country will be under real debate.\textsuperscript{534} Abu Bakar Munir states that a privacy authority has to be independent; however, in Malaysia, Munir argues that the independence of the Personal Data Protection Commissioners is absent because those commissioners are answerable to the minister.\textsuperscript{535} Munir claims that ‘the problem with this is that the Commissioner may not be able to enforce the Act effectively without fear or favour unlike in other countries’.\textsuperscript{536}

The Malaysian law has a number of limitations with regards to the independence of commissioners. These limitations can obviously be seen from ss 54, 57, 60 of the \textit{Malaysian Personal Data Protection Act (2010)}:

\begin{itemize}
  \item \textsuperscript{531} \textit{Personal Data Protection Act 2010 (Malaysia)}, s 47.
  \item \textsuperscript{532} Ong, above n 278, 433.
  \item \textsuperscript{533} \textit{Personal Data Protection Act 2010 (Malaysia)}, s 59.
  \item \textsuperscript{535} Abu Bakar Munir cited in Habib, above n 324.
  \item \textsuperscript{536} Ibid.
\end{itemize}

152
1- The minister, who is charged with the responsibility for the protection of personal data, has the power to revoke the appointment of the Commissioner by stating the purpose for such revocation. This power might lead the Commissioner to follow the views of the minister regarding any matter, to prevent any clash with the minister.

2- The minister, by consultation with the minister of finance, decides the remuneration and allowances that should be given to the commissioners. This reflects how the commissioners will be financially dependent on the funding that is determined by the government authority.

3- The minister has the authority to require any reports or accounts regarding the functions of the commissioners. This apparently reduces transparency and integrity as the minister will receive any reports from the commissioners and if there is any debate regarding reports, the minister can conceal these reports and prevent such documents and reports being distributed publicly.

With regards to the lack of independence and transparency of Personal Data Protection Commissioners in Malaysia, Rebecca Ong claims that

It is clear that this lack of independence is a critical deficiency in the Act as not only does it undermine the integrity of the data protection law, it also weakens the protection of the individuals’ data privacy. A Commissioner must not only be free from any external influence, including the direct or indirect influence of the state but must also be seen to be free from such influences. There is no doubt that a mere risk or possibility of political influence through state scrutiny is sufficient to hinder the independent performance of the supervisory authority’s tasks.

Ong clearly criticizes the process of appointing a commissioner to the supervisory authority and the serious setback to the independence of the agency because the commissioners are responsible to the minister. The commissioners should be free

---

537 Personal Data Protection Act 2010 (Malaysia), s 4.
538 Personal Data Protection Act 2010 (Malaysia), s 54.
539 Personal Data Protection Act 2010 (Malaysia), s 57.
540 Personal Data Protection Act 2010 (Malaysia) s 60.
541 Ong, above n 278, 433.
from any intervention of the government authorities in order to perform with integrity and transparency.

B. The Moroccan Data Protection Commission

*Personal Data Protection Act 2009* (Morocco) introduces a Data Protection Authority and this supervisory authority has the power to carry out and enforce the principles of data protection law.\textsuperscript{542}

The Moroccan data protection law gives the right to the king of Morocco to appoint the head of the Data Protection Commission. The other commissioners will be appointed by the king with recommendations from the prime minister or the head of parliament.\textsuperscript{543} The Moroccan government will appoint a ‘public servant’ who will be responsible for financial and administrative matters to work with the commissioners in the supervisory authority. This public servant will help the commissioners with the preparation and implementation of the budget of the supervisory agency.\textsuperscript{544}

It should be noticed that the head of the Moroccan Data Protection Authority will be chosen by the king of Morocco. Such a process to appoint the president of the committee might affect the independence of such an agency because there might be a conflict of views between the vision of the commissioners and the Moroccan government. Data commissioners might lose their independence as the king of Morocco may change the head of commissioners when there is a clash of views.

Another weakness of the independence of the commissioners is that an employee who works for the government has the responsibility for preparing the budget for the commissioners. This kind of dependence on government funding might negatively affect the performance of the Data Protection Commission.

Upon the formation of privacy legislation in Morocco and Malaysia, it is obvious that those two countries do not follow the requirements of establishing independent Data Protection Authorities which have been provided by many international

\textsuperscript{542} See *Personal Data Protection Act 2009* (Morocco) s 27- s31.

\textsuperscript{543} *Personal Data Protection Act 2009* (Morocco) s 32.

\textsuperscript{544} *Personal Data Protection Act 2009* (Morocco) s 40.
resolutions. The Libyan policy-makers should consider such limitations and try to find a legal basis to ensure the independence and credibility of any proposed supervisory agency.

5.1.3.3 The creation of the Libyan Data Protection Commission

In order to study the creation of a Libyan data protection authority, this section will first provide summary of the common requirements for establishing DPAs; second examine the Supreme Commission of Applying the Required Standards for Holding Public Positions and third the benefits of following the precedent of the Supreme Commission in establishing a Libyan Data Protection Commission.

1. Summary of the common requirements for establishing DPAs from other jurisdictions

Libya, in order to establish Data Protection Commission, should learn from the practice of other nations and try to build on them with some enhancements. Graham Greenleaf studied the practice of Data Protection Commission in different Asia-Pacific jurisdictions such as Australia, Thailand, Malaysia and South Korea. Greenleaf notices some requirements which are very common in forming independent data protection commissioners for the Pacific countries that include supervisory authority in their laws. These attributes of independence are as follows:

1- Independence guaranteed by legislation, giving the ability to investigate free of direction;

2- Appointment of commissioners for a fixed term;

3- Removal only for specified inadequate conduct, usually only by the legislature;

4- Ability to report directly to the public and to the legislature through an Annual Report, at least;

5- Forbidden to hold other concurrent positions;

6- A right of appeal against data protection authorities’ decisions.545

545 Greenleaf, above n 461, 127.
In addition to the above requirements Greenleaf noticed other less common attributes of independence in the laws of the Asia-Pacific countries with regard to data protection commissioners. Some of these requirements are:

1- Appointment by the legislature rather than the executive;
2- Resources determined independently of the executive;
3- Immunity against personal law suits arising from a commissioner’s conduct of office;
4- Prohibition on commissioners with conflicting interest or a requirement to disclose.\textsuperscript{546}

It is clear that these requirements will contribute to the independence of the supervisory institution because such requirements would play a vital role in ensuring the independence of data protection commissioners from the government, in terms of political and financial interference. The Libyan policy-makers, when they come to establish a Data Protection Commission, should consider such requirements as it is important to gain experience from the practices of different legal jurisdictions.

The roles of supervisory authorities according to the practices of different jurisdictions have been explained above and it is clear that data protection commissioners commonly have quasi-judicial powers in terms of investigating complaints and imposing fines. Thus, a Libyan supervisory agency should meet specific requirements to guarantee that it would perform impartially and effectively.

The next subsections will examine the Supreme Commission by considering its establishment and then will analyse the significance of establishing Data Protection Commission by following the same criteria of establishing the Supreme Commission.

2. The Supreme Commission of Applying the Required Standards for Holding Public Positions

The proposed Data Protection Commission in Libya should take into consideration the establishment of the Supreme Commission of Applying the Required Standards for Holding Public Positions which is responsible for applying the Political and Administrative Isolation law in Libya. The Supreme Commission has been

\textsuperscript{546} Ibid.
established by meeting special requirements which reflect credibility, integrity and independence. Therefore, the Libyan Data Protection Commission might be created in a similar way as the Supreme Commission.

The Political and Administrative Isolation Law no 13 (2013) (Libya) aims to prevent persons who worked with the former Libyan regime in specific positions (1969 to 2011) from taking higher positions in the country for 10 years. In order to implement the law, art 3 introduces a new commission that is responsible for applying the Political and Administrative Isolation Law under the name ‘the Supreme Commission of Applying the Required Standards for Holding Public Positions’. This Commission has been given legal personality and also financial independence.

Article 4 of the Libyan Political Isolation Law gives the High Judicial Council the right to nominate the members of the Commission who are responsible for applying the law and obtaining approval from the parliament.

According to the law, no 4 (2011) amends the law no 6 (2006) which organises the judiciary system in Libya. The High Judiciary Council comprises

1- The President of the Supreme Court (The president)
2- The Attorney-General (The deputy president)
3- The Presidents of the Courts of Appeal (Members).

The requirements that the members of the Supreme Commission should meet are introduced by the Political Isolation Law and accordingly, the members are required to meet the following conditions:

1- Must hold Libyan nationality.
2- Must be known for their honesty.
3- Must not be less than 35 years of age.
4- Must not be convicted of any criminal offence or felony relating to honour.

547 Political and Administrative Isolation Law no 13 (2013) ss 1, 18.
548 Political and Administrative Isolation Law no 13 (2013) s 3.
549 Law no 4 (2011) amends the law no 6 (2006) which organises the judiciary system, s 3.
5- Must not have been dismissed from any position except for political reasons.

6- Must not be affiliated with any political entity or party.

7- Must have an academic degree in law [or higher degree].

The Supreme Commission has the power to determine its budget independently and the President of the Commission provides the proposed budget to the parliament to be approved.

The Libyan Political Isolation Law endorses that the Chairperson and members of the entity, who are responsible for applying the law, will be subject to the provisions of Law no 6 of 2006 which organises the Libyan judiciary system in respect of disciplinary actions, investigations, and the filing of criminal lawsuits. This means that the members of the agency will gain the same legal protection as is given to the judges.

The Political Isolation Law gives the members of the Supreme Commission a judicial immunity granted to judges so that no criminal suit may be brought against them, unless there is an approval from the parliament. The Libyan Political Isolation Law gives persons the right to appeal against any decision made by the Supreme commission that is responsible for applying the Political Isolation Law. The appeal must be brought to the Court of Appeal within ten days of those persons receiving the announcement.

3. The benefits of following the precedent of the Supreme Commission in establishing a Libyan Data Protection Commission

There are many benefits that can be gained if a Data Protection Authority in Libya is established by following the practice of the creation of the Supreme Commission of Applying the Required Standards for Holding Public Positions. These advantages are as follows:

550 Political and Administrative Isolation Law no 13 (2013) s 5.
551 Political and Administrative Isolation Law no 13 (2013) s 7.
554 Political and Administrative Isolation Law no 13 (2013) s 12.
Firstly, the independence of the Data Protection Authority will be guaranteed when those commissioners are chosen by following a process similar to the appointment of the members of the Supreme Commission. The independence of those commissioners can be seen as follows:

A- Nomination by the High Judiciary Council and then obtaining approval from the legislative body. This reflects the independence of commissioners because the government in this situation does not play any role in choosing the commissioners. Therefore, the commissioners will be able to make their decisions depending on the subjective elements of the matters, without any external intervention from the government or other organisations.

B- The independence to determine the budget. The political isolation law stipulates that the Supreme Commission will be independent in terms of determining its budget which should be approved by the parliament. This means that the Supreme Commission will not be financially dependent on the government. Thus, the Data Protection Authority should also be given this power to guarantee its independence.

Secondly, judicial immunity must be given to the commissioners of Data Protection Authority. The political isolation law gives the Supreme Commission members a judicial immunity granted to the judges. This judicial immunity will guarantee that the commissioners of Data Protection Authority will work without any fear that they might be sued unless there is an approval from the parliament. This protection will lead the commissioners to perform effectively in doing their work without any fear of legal action being taken against them.

Thirdly, the requirements that the members of the Supreme Commission must meet ensures enough credibility so the same requirements might be adopted in choosing the commissioners for the Data Protection Authority. These requirements include that

- They are known for their honesty;
- There are no judicial decisions enforced on them for criminal offences;
- They do not join any political parties;
They have not been dismissed from their previous job, unless for political reasons.

These requirements might contribute to the commissioners successfully applying privacy law because they will be chosen according to specific standards.

Fourthly, if the process of creating the Supreme Commission is adopted in establishing the Data Protection Commission, the commissioners will only be revoked according to the conditions which are stipulated in *Law No 6 of 2006*. This law organises the Libyan judiciary system in respect of disciplinary actions, investigations and the filing of criminal law suits against judges.

It is clear that by following the above requirements, the Libyan Data Protection Commission will almost meet the requirement of independence. If the Libyan supervisory agency is established as the Supreme Commission has been established, the commissioners will perform their duties effectively and independently from any external interference. The only requirement that should be added is that the commissioners responsible for monitoring the application of privacy law should be appointed for a fixed term.

The Libyan authorities should take into consideration the requirements for achieving independence and transparency when forming the supervisory authority. By following the above proposal for establishing a Data Protection Commission, the Libyan data protection commissioners will be strong in terms of investigating complaints and imposing fines. The adoption of the above mentioned requirements will prevent Libya from suffering the same limitations that appeared in the establishing of Data Protection Authorities in Malaysia and Morocco. It is obvious that in those two countries, the independence of commissioners politically and financially from the government is absent.

**Recommendation 5.9:** the Libyan Data Protection Commission should be established in the same way as the Supreme Commission of Applying the Required Standards for Holding Public Positions has been established.
5.2 Remedies and sanctions for contravening data protection law

All data protection laws provide different types of sanctions and remedies when there is a violation of their principles. The provisions which consider sanctions and remedies generally provide for a combination of penalties (fines and imprisonment) and compensatory damages. The next discussion will examine remedies and sanctions by considering the approach of different legal systems.

5.2.1 Remedies

There is a clear need for useful remedies which should be implemented when there are breaches of privacy provisions with regard to the processing of personal information. These remedies would ensure that data controllers, when they process personal information, are abiding by the principles of privacy law and if that does not happen, the aggrieved person will ask for redress of his or her rights.

The enforcement notice instructions by data protection commissioners and the court orders seem to be vital to remedy any breach of personal information principles as these orders aim to force data controllers to follow their obligations under the law. The other type of remedy is giving compensation to redress the damages that individuals suffer as a result of the breaches of their privacy.

5.2.1.1 Data Protection Commission orders

Commonly, when there is a contravention of privacy law, Data Protection Authorities firstly bring a notice known as an ‘enforcement notice’ which orders data controllers to comply with data protection law and forces companies or organisations that deal with personal information to correct their activities. The enforcement

555 Bygrave, above n 515, 77.
556 South African Law Reform Commission, above n 471, ch 6, 4.
557 Ibid ch 6, 2.
558 Data Protection Act 1998(UK) s 40 provides some instructions that the commissioners will force data controllers to follow in order to redress their breach of personal data. The law provides that:

(1)If the Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commissioner may serve him with a notice (in this Act- referred to as “an enforcement notice”) requiring him, for complying with the principle or principles in question, to do either or both of the following—
notice usually requires data controllers to follow the instructions that are provided by
the commissioners which aim to correct their actions. Enforcement notices require
data controllers to take some steps to remedy the breach by destroying, rectifying and
blocking any inaccurate data.\textsuperscript{559} Data protection commissioners may cancel or vary

\begin{itemize}
\item[(a)] to take within such time as may be specified in the notice, or to refrain from taking
after such time as may be so specified, such steps as are so specified, or
\item[(b)] to refrain from processing any personal data, or any personal data of a description
specified in the notice, or to refrain from processing them for a purpose so specified or
in a manner so specified, after such time as may be so specified.
\end{itemize}

(2) In deciding whether to serve an enforcement notice, the Commissioner shall
consider whether the contravention has caused or is likely to cause any person damage
or distress.

(3) An enforcement notice in respect of a contravention of the fourth data protection
principle which requires the data controller to rectify, block, erase or destroy any
inaccurate data may also require the data controller to rectify, block, erase or destroy
any other data held by him and containing an expression of opinion which appears to
the Commissioner to be based on the inaccurate data.

(4) An enforcement notice in respect of a contravention of the fourth data protection
principle, in the case of data which accurately record information received or obtained
by the data controller from the data subject or a third party, may require the data
controller either—

\begin{itemize}
\item[(a)] to rectify, block, erase or destroy any inaccurate data and any other data held by him
and containing an expression of opinion as mentioned in subsection (3), or
\item[(b)] to take such steps as are specified in the notice for securing compliance with the
requirements specified in paragraph 7 of Part II of Schedule 1 and, if the Commissioner
thinks fit, for supplementing the data with such statement of the true facts relating to the
matters dealt with by the data as the Commissioner may approve.
\end{itemize}

(5) Where—

\begin{itemize}
\item[(a)] an enforcement notice requires the data controller to rectify, block, erase or destroy
any personal data, or
\item[(b)] the Commissioner is satisfied that personal data which have been rectified, blocked,
erased or destroyed had been processed in contravention of any of the data protection
principles—

an enforcement notice may, if reasonably practicable, require the data controller to
notify third parties to whom the data have been disclosed of the rectification, blocking,
erasure or destruction; and in determining whether it is reasonably practicable to require
such notification regard shall be had, in particular, to the number of persons who would
have to be notified.
\end{itemize}

(6) An enforcement notice must contain—

\begin{itemize}
\item[(a)] a statement of the data protection principle or principles which the Commissioner is
satisfied have been or are being contravened and his reasons for reaching that
conclusion, and
\item[(b)] particulars of the rights of appeal conferred by section 48.
\end{itemize}

\textsuperscript{559} Ibid.
an enforcement notice.\textsuperscript{560} Penalties apply on data controllers for failure to comply with the requirements of enforcement notice.\textsuperscript{561} Data controllers have the right to appeal against the notice.\textsuperscript{562}

For instance, the \textit{Malaysian Personal Data Protection Act 2010} introduces the enforcement notice as a procedure to guarantee that data controllers fulfil the Act. The law stipulates that

(1) Where, following the completion of an investigation about an act, practice or request specified in the complaint, the Commissioner is of the opinion that the relevant data user:

(a) is contravening a provision of this Act; or

(b) has contravened such a provision in circumstances that make it likely that the contravention will continue or be repeated,

Then the Commissioner may serve on the relevant data user an enforcement notice:

(A) stating that he is of that opinion;

(B) specifying the provision of this Act on which he has based that opinion and the reasons why he is of that opinion;

(C) directing the relevant data user to take such steps as are specified in the enforcement notice to remedy the contravention or, as the case may be, the

\textsuperscript{560} \textit{Data Protection Act} 1998 (UK) S 41 under title “Cancellation of enforcement notice” stipulates that

(1) If the Commissioner considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the data protection principle or principles to which it relates, he may cancel or vary the notice by written notice to the person on whom it was served.

(2) A person on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal can be brought against that notice, apply in writing to the Commissioner for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the data protection principle or principles to which that notice relates.

\textsuperscript{561} \textit{Personal Data Protection Act} 2010 (Malaysia) s 108 (8) stipulates that ‘[a] person who fails to comply with an enforcement notice commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both’. \textit{Data protection Act} 1998 (UK) S 47 stipulates that ‘[a] person who fails to comply with an enforcement notice is guilty of an offence’ that means s 60 of the act which enforce penalties on offenders will apply.

\textsuperscript{562} See \textit{Data Protection Act} 1998 (UK) S 48 with gives data controller the right to appeal against the notice to the tribunal. The Malaysian \textit{Personal Data Protection Act} (2010) s 108 (6) gives data controller the right to appeal to Appeal Tribunal against the enforcement notice.
The above provision of the Malaysian law offers an enforcement notice which suggests some steps that ‘data controllers’ should follow to remedy the contravention of the Act.

**Recommendation 5.10: privacy law should give data protection commissioners the power to use enforcement notices in order to address any infringement to the Act.**

### 5.2.1.2 The court orders to redress privacy breach

In addition to the enforcement notice by data commissioners, the court has the power to make orders to redress any contravention of the privacy Act. The *EU Directive* gives the right for any person to seek remedy through the court. The *EU Directive* states that ‘member States shall provide for the right of every person to a judicial remedy for any breach of the rights’.  

The court can order data controllers to follow data protection principles. For instance, in the circumstances of processing personal data the *Data Protection Act 1998* (UK) requires data controllers to provide data subjects with a description regarding the purposes of processing their personal data and the recipients or classes of recipients to whom personal data is disclosed.  

*Data Protection Act 1998* (UK) gives the court, if it is satisfied that the data controller has failed to comply with such requirements, the power to order data controllers to comply with the request.

*Data Protection Act 1998* (UK) stipulates some circumstances where the court has the powers of rectification, blocking, erasure and destruction of personal data. Some of these orders are stipulated in s 14(1) (4).  

---

563 *Personal Data Protection Act 2010*(Malaysia) s 108(1).  
564 *EU directive* 95/46 EC, art 22.  
565 *Data Protection Act 1998* (UK) s 7(1)  
566 *Data Protection Act 1998* (UK) s 7(9).  
(1) If a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contain an expression of opinion which appears to the court to be based on the inaccurate data.

(4) If a court is satisfied on the application of a data subject

(a) that he has suffered damage by reason of any contravention by a data controller of any of the requirements of this Act in respect of any personal data, in circumstances entitling him to compensation under section 13, and

(b) that there is a substantial risk of further contravention in respect of those data in such circumstances,

the court may order the rectification, blocking, erasure or destruction of any of those data.

The Libyan policy-makers should consider the value of providing a variety of powers to enforce remedies either to the data protection commissioners or to the courts. These orders aim to rectify any unlawful activity with the personal information of individuals and to provide strong protection to individuals whose data is at risk.

**Recommendation 5.11: the court should be given the power to enforce orders that aim to redress any offences by data controllers.**

### 5.2.1.3 Compensation

Another significant type of remedy is that an individual who suffered damages as a result of a privacy infringement can seek compensation through the courts. Any person who suffers damages caused by breaches of his or her privacy can gain compensation as a remedy.\(^{568}\) The liable person might be a data controller or another person who breaches data protection law. The aggrieved person has to prove that the action of the data controller has caused damage to him or her.\(^{569}\) It is clear that ‘compensation is intended to place the individual in the position which he would have been in apart from the wrong which has been done. It is not intended to be punitive’.\(^{570}\) The *EU Directive* stipulates that

---

\(^{568}\) Jay, above n 367, 469.

\(^{569}\) Ibid.

\(^{570}\) Ibid 470.
[m]ember States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.\textsuperscript{571}

The \textit{EU Directive} gives data controllers the right to defend themselves from being liable if they can provide evidence which supports that they are not responsible for the damage.\textsuperscript{572}

It is clear that the \textit{EU Directive} ensures the right for every individual to obtain civil remedies when their privacy right is breached.

\textit{Data Protection Act 1998(UK)} adopts the above mentioned article of the \textit{EU Directive} in s 13 under the title ‘Compensation for failure to comply with certain requirements’. The law stipulates that:

(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.\textsuperscript{573}

The Libyan policy-makers should recognise the importance of introducing civil remedies for the effectiveness of privacy law. These remedies will protect data subjects where there is any breach of their personal information. The strong redress mechanism ensures that data controllers will consider the issue of data protection seriously and take into consideration the procedures to protect the subject of personal data. It is suggested above that some of these remedies that can contribute to the effectiveness of data protection law and it is believed that there might be other types of redress which can be included to provide stronger protection of personal information.

\textsuperscript{571} \textit{EU Directive} 95/46 EC art 23(1).
\textsuperscript{572} \textit{EU Directive} 95/46 EC, art 23.
\textsuperscript{573} \textit{Data Protection Act 1998(UK)}, s 13(1)-(3).
Recommendation 5.12: the law should ensure that any person who suffers damage when a data controller infringes the law is entitled to compensation from the data controller.

5.2.2 Sanctions

Sanctions are the punishments that will be enforced on data controllers who have broken the principles concerning the process of treating personal data. It is said that ‘in investigation or audit programs, the use of formal powers, and the imposition of sanctions at a national level, could turn out to be necessary’.\(^{574}\)

The next subsections will examine two types of sanctions, civil monetary penalties by Data Protection Authorities and criminal penalties (imposing fines and imprisonment).

5.2.2.1 Civil monetary penalty

In order to settle any privacy matters, supervisory authorities might in some circumstances enforce some penalties against the processors of personal data. The UK data protection law takes this direction. The UK act offers to the commissioners the power to impose monetary penalties. The law stipulates that

\[(1)\] The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that

(a) there has been a serious contravention of section 4(4)\(^{575}\) by the data controller;

(b) the contravention was of a kind likely to cause substantial damage or substantial distress.

\[(2)\] This subsection applies if the contravention was deliberate.

\[(3)\] This subsection applies if the data controller

(a) knew or ought to have known

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

---

\(^{574}\) EU Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, above n 450, 3.

\(^{575}\) Section 4 (4) Data Protection Act 1998 (UK), provides that ‘it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller’.

167
The UK Information Commissioner Office can impose penalties up to £500000 for infringing Data Protection Act. Data controllers are given the right to appeal against the monetary penalties to First-tier Tribunal (Information Rights).

Similarly, the Data Protection Authority in France has the power in some circumstances to enforce financial penalties of ‘a maximum amount of 150000 Euros and where similar previous offences have been committed, an amount of up to 300000 Euros’. The monetary penalties are collected by the French Treasury and not by the CNIL.

The next two examples from Data Protection Authorities in France and UK show how these authorities enforce financial penalties on offenders who infringe data protection law.

In 2011, the French Data Protection Authority (CNIL) imposed a fine of €100000 on Google for infringing the French Data Protection Act. CNIL discovered that Google violated the French law in many circumstances such as ‘collecting Wi-Fi data without the knowledge of the data subjects and the recording of data relating to content (IDs, passwords, login details, email exchanges).

In 2012, the UK Information Commissioner Office enforced a Civil Monetary Penalty (CMP) of £325000 on Brighton and Sussex University Hospitals NHS Trust as a result of their serious violation of the UK Data Protection Act. It was discovered...

---

576 Data Protection Act 1998 (UK), s 55A.
578 Ibid.
580 Ibid.
that sensitive personal data related to thousands of patients and staff, had been stored on hard drives and sold on an Internet auction site.\textsuperscript{582}

David Smith, the Deputy Commissioner of the UK Information Commissioner Office and Director of Data Protection, held that ‘the amount of the CMP [Civil Monetary Penalty] issued in this case reflects the gravity and scale of the data breach. It sets an example for all organisations - both public and private - of the importance of keeping personal information secure’.\textsuperscript{583}

The Libyan policy-makers may give the commissioners the right to enforce monetary sanctions or penalties on offenders who breach the privacy of individuals. Such a role may increase confidence in implementing the law as offenders will take into account such penalties before committing an offence.

| Recommendation 5.13: data protection authority might be given the power to enforce civil monetary penalty in some circumstances where there is breach to privacy law. |

\textbf{5.2.2.2 Criminal penalties}

Only some jurisdictions provide for civil monetary penalties which are imposed by the data protection authority. It is more common for fines to be included in criminal enforcement provisions enforced by the judicial system. It is important that some penalties exist for breach of data protection principles in order to deter future breaches. While civil monetary penalties can provide an important way for data protection authorities to increase compliance with the law, it is likely to be important to supplement these measures with criminal provisions for more serious breaches.

\textbf{1. Imposing Fines}

Enforcing fines on persons who breach data protection law is one of the sanctions that aim to deter persons from further breaches. The majority of data protection laws


\textsuperscript{583} Ibid.
enforce fines when there are breaches of personal data which are committed by data controllers. The UK data protection law imposes fines on persons who are guilty of an offence under any provision of the Act.\textsuperscript{584}

The Malaysian law enforce fines on persons who commit offences under the provisions of the Act. For example, the law provides that a data controller who transfers personal data to places outside Malaysia that do not provide adequate protection to personal data commits an offence and shall be liable to sanctions. A fine not exceeding three hundred thousand ringgit is one of the penalties that would be enforced.\textsuperscript{585}

Similarly, the Moroccan data protection law imposes fines on data controllers when they fail to obey the requirements of the law in terms of processing personal data. The Moroccan Act distinguishes the offences committed by data controllers and provides specific sanctions for each offence. The fines can be up to 300 000 Dirham.\textsuperscript{586}

The Libyan policy-makers should consider that there is real value in imposing fines for reducing or preventing further offences. The law should stipulate a variety of monetary sanctions on persons who commit offences because these fines may have a positive effect on public confidence as the public will trust that data protection law will impose fines on guilty persons when their personal information is breached.

\textbf{Recommendation 5.14: the law should ensure that fines are enforced on offenders who breach the law.}

\section{2. Imprisonment}

Many data protection laws introduce imprisonment as sanctions on offenders who breach the law. For instance, The Malaysian law introduces prison sentences for data users who fail to comply with the principles of the data protection law and fail to

\textsuperscript{584} Data Protection Act 1998 (UK) S 60.

\textsuperscript{585} Personal Data Protection Act 2010 (Malaysia) s 129 (1) (5). See other provisions like ss 5, 16, 29 and 37 of the act.

\textsuperscript{586} Personal Data Protection Act 2009 (Morocco) ss 52, 53, 60.
correct the wrongdoing.\textsuperscript{587} For example, the law stipulates that data users who fail to take some steps, which are required by the data protection commissioners to remedy the contravention of privacy law\textsuperscript{588} will commit an offence and may be sentenced to imprisonment for a period not exceeding two years.\textsuperscript{589}

Similarly, the \textit{Personal Data Protection Act 2009} (Morocco) endorses prison sentences on persons who fail to comply with the provisions of the law. There are many provisions that enforce jail sentences which range from 3 months to two years, depending on the type of offences that were committed.\textsuperscript{590}

The situation in the UK is different to the abovementioned legislation. The \textit{UK Data Protection Law 1998} does not provide imprisonment for infringing privacy law. There is current debate in the UK considering the introduction of custodial sanctions.\textsuperscript{591}

The lack of imprisonment as a potential sanction has been criticised in the UK. The UK Information Commissioner’s office argues that evidence, which is gathered by the office, indicates

a flourishing and unlawful trade in confidential personal information by unscrupulous tracing agents and corrupt employees with access to personal information. Not only is the unlawful trade extremely lucrative, but those apprehended and convicted by the courts often face derisory penalties.\textsuperscript{592}

The UK Department of Constitutional Affairs states that ‘the government is clear that prison should be reserved for serious, violent and dangerous offenders. For other

\begin{itemize}
\item[587] \textit{personal data protection act 2010} (Malaysia) s 108 (8).
\item[588] \textit{Personal Data Protection Act 2010} (Malaysia) s 108(1).
\item[589] \textit{Personal Data Protection Act 2010} (Malaysia) s 108 (8). See also another example in s 5 (2) of the act.
\item[590] \textit{Personal Data Protection Act 2009} (Morocco), S 52-63.
\end{itemize}
offenders, the courts have available a range of tough non-custodial sentences such as fines and community sentences.

The report of the UK Justice Committee criticises the current UK data protection law as there are no imprisonment sanctions for offences under s 55. The Justice Committee argues that

It is clear to us that the current penalties for section 55 offences are inadequate. If people can make more money from a single offence than the fine which would be imposed for such an offence, then there is no deterrent. There are also cases where people have been endangered by the data disclosed, or where the intrusion or disclosure was particularly traumatic for the victim, and a fine is not an adequate sentence.

---

593 The UK Department of Constitutional Affairs, above n 591, 14.

594 Section 55 of the Data Protection Act 1998 (UK) stipulates that:

1. A person must not knowingly or recklessly, without the consent of the data controller—
   - obtain or disclose personal data or the information contained in personal data, or
   - procure the disclosure to another person of the information contained in personal data.
2. Subsection (1) does not apply to a person who shows—
   - that the obtaining, disclosing or procuring—
     - was necessary for the purpose of preventing or detecting crime, or
     - was required or authorised by or under any enactment, by any rule of law or by the order of a court,
   - that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person,
   - that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it, or
   - that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.
3. A person who contravenes subsection (1) is guilty of an offence.
4. A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).
5. A person who offers to sell personal data is guilty of an offence if—
   - he has obtained the data in contravention of subsection (1), or
   - he subsequently obtains the data in contravention of that subsection.

The Information Commissioner states that the Office objective is to discourage this illegal trade. In order to achieve its aim, the Commissioner’s Office suggests that severe penalties should be provided. The introduction of a custodial sentence can ‘underline the seriousness of the offence and make reputable businesses and individuals reflect on the possible consequences of their actions’.596 Thus, The Information Commissioner recommends an amendment to s 60(2) of the Data Protection Act 1998. This amendment will increase the punishment for s 55 offences by enforcing imprisonment sanctions not exceeding two years.597

The UK government believes that it is essential to increase the penalties available to the courts for the following reasons:

1. in order to provide a larger deterrence to those who seek to knowingly or recklessly disclose or procure the disclosure of confidential personal information without the consent of the data controller;

2. to provide public reassurance that those who are successfully prosecuted may, dependent on the gravity of the offence, be sent to jail.598

Christopher Graham, the UK Information Commissioner, said that ‘[u]nscrupulous individuals will continue to try and obtain peoples’ information through deception until there are strong punishments to fit the crime. We must not delay in getting a custodial sentence in place for s 55 offences under the Data Protection Act’.599

It is understood that there is strong support for introducing prison sentences for serious offences because severe punishments will contribute to reducing potential offences. The Libyan policy-makers should consider the abovementioned issues considering sanctions. Thus, the Libyan legislators should consider prison sentences where there is serious contravention of personal information.

Prison sentences would play an effective role in public deterrence because custodial sanctions would be considered as severe punishment so those who attempt, for

596 The UK Information Commissioner office, above n 592, 29.
597 Ibid.
598 The UK Department of constitutional affairs, above n 591, 10.
example, to sell or misuse personal information may take into account that if they are found guilty, they might be sentenced to jail.

It seems that in Libya, it may be important to consider introducing strong penal sanctions in order to deter any potential offenders who may infringe the principles of privacy law. Punishments might have a deterrent effect in one of two ways

1. First, by increasing the certainty of punishment, potential offenders may be deterred by the risk of apprehension. Second, the severity of punishment may influence behaviour if potential offenders weigh the consequences of their actions and conclude that the risks of punishment are too severe.

It is clear that punishments have positive effects in the way that potential offenders may consider the outcome - a fine or prison - of their offences before they commit an offence.

To conclude this section, it is noteworthy to mention the EU Report on ‘a comprehensive approach on personal data protection in the European Union’ which considers the issue of increasing the effectiveness of remedies and sanctions. The EU Report states that to apply data protection law successfully, there is a need that the law introduces strong sanctions and remedies which will be enforced when there is any breach of data protection law. The importance of providing severe punishments for offenders and particularly, introducing criminal sanctions in the circumstances of serious breaches of privacy law, should be taken in to account.

**Recommendation 5.15: the law should force prison sentences on offenders who breach the law.**

---


602 Ibid.

603 Ibid.

174
5.3 Conclusion

This chapter examined the issue of privacy enforcement by studying firstly Data Protection Commission with regard to their powers, functions and the requirements that it should meet in order to work effectively, and secondly, remedies and sanctions which are enforced on people who contravene personal information.

To enforce privacy law, there is a need to first establish a Data Protection Commission in Libya, as suggested in this chapter. This supervisory authority should be given the power and functions to perform effectively and play a vital role in implementing the law. The commissioners of Data Protection Authority should provide their reports to the public and explain the reasons behind their decisions, to guarantee transparency. Secondly, the data protection law should include remedies and sanctions which should be severe enough to deter potential offenders from infringing the law. These sanctions might be varied depending on the type of offences that are committed.
Chapter VI Conclusion

This thesis considered the issue of information privacy protection from a Libyan perspective. The aim was to find a privacy system that could be applicable in Libya. Because the principles of Sharia law are considered by the Libyan Constitutional Declaration (2011) as the main source of legislation in Libya, it was important to examine the right to privacy according to an Islamic perspective. The main reason to evaluate the direction of Sharia law was to recognise how Sharia values the right to privacy. The study found that the right of individuals’ private life is under strong protection: it is considered as one of the most valued rights linked to persons. This strong protection of privacy in Sharia accords well with international conventions which view privacy as a human right. This finding suggests that the Libyan policy-makers may choose any system of privacy protection, as long as this system values the right to privacy and sufficiently defends personal information.

This thesis aimed to find a strong model that would provide powerful protection to personal information. Two approaches to data protection have been examined in this study: the self-regulatory model and the legislative approach. It found that the self-regulatory model of privacy protection does not provide sufficiently strong protection to personal data. The practice of the US self-regulatory model to data protection has a number of limitations, in particular in terms of transparency and accountability. Further, the experience of developing countries which have adopted the self-regulatory approach in some parts of business, such as in voluntary environmental protection, indicates the weakness of such a model in developing countries. In particular, developing countries may lack strong consumer groups who are able to enhance and encourage a voluntary model by pressuring firms and organisations to follow their business standards. This weakness of consumer pressure in developing countries is clearly linked to the lack of consumers’ education and knowledge regarding their obligations and rights.

The thesis argued that in order to have a strong protection for individuals regarding their personal data, a legislative approach should be the model adopted by the Libyan policy-makers. The reason for suggesting this approach is because this model
requires comprehensive protection for individuals with regard to matters related to privacy such as transferring, sharing, and securing personal data.

Next, this thesis considered the common features of substantive privacy regimes. Commonly, data protection laws provide fair information principles which any firms or organisations should follow. Fair information principles give data subjects more control of their personal data and enforce some obligations on data controllers considering the processing of personal data. The thesis examined some of the privacy principles which consider the processing of transferring or sharing personal information and these principles are derived from the practices of different jurisdictions.

Furthermore, the thesis examined the enforcement of data protection law. Usually, any data protection laws demand a strong mechanism for enforcing privacy principles. Creating Data Protection Authorities, imposing remedies and enforcing sanctions are the methods that the majority of privacy laws implement. Following such mechanisms makes the implementation of data protection principles effective and successful.

In order to assist the Libyan policy-makers to find an applicable system of data protection, the following recommendations will provide guidelines which lay down some priorities that the Libyan policy-makers should consider to increase the level of privacy protection and reduce data subjects’ concerns:

- Introduce data protection law as soon as possible following the international direction followed by the majority of countries which have enacted privacy laws. As concluded in this thesis, the legislative approach, as a method of defending personal data, provides strong and comprehensive protection for personal data. Privacy is a fundamental human right that should be under real protection by law and it should not be left to firms or organisations to devise their principles to protect their clients’ privacy. The Libyan policy-makers should gain experience from the practice of other legislation and in particular the implementation of privacy laws in developing countries such as Malaysia and Morocco. The benefit from examining these laws is to ensure the Libyan policy-makers do not face the same obstructions that these laws have faced.
• The Libyan policy-makers should include consumer advocates’ groups, firms and organisations in the process of forming data protection law because such dialogue will guarantee that the law will reflect public opinion. The goal of data protection law should be to achieve a balance between the right of data subjects to have their rights sufficiently protected and the need of data controllers to gain benefits from sharing personal data and accordingly, to not be negatively affected by such law.

• Organisations and firms should be given a transitional period in order to comply with the new law. This is very important because it is not easy for data controllers to comply immediately with new principles regarding the processing of personal data. During this transitional period, data controllers have to prepare their operations to comply with the new legislation: for example, change their default system from the opt-out format to the opt-in format when the legislation requires such obligations.

• In order to enact privacy law, the Libyan legislators should take into consideration the practice of the EU Directive 95/46 EC and the OECD Guidelines regarding their approach to protecting personal data as the majority of data protection laws have considered those directions when forming their own data protection law. The international standards will assist any policy-makers to establish strong legislation as the Directive and the Guidelines are a result of a comprehensive studies and proposals. Therefore, it is vital to examine and consider such standards and try to apply the principles that are relevant to the Libyan perspective.

Data protection law should be clear in defining the terms which affect on implementing the law. With regard to provide some exceptions to the scope, the law must be clear and not broad. In particular the thesis recommends that:

**Recommendation 4.1:** a broad approach to defining personal data should be adopted.
**Recommendation 4.2:** Data protection Act should apply to natural persons and should not apply to corporations or organisations.

**Recommendation 4.3:** Data protection law should be applicable only to living persons, but the law may include the protection of deceased persons in exceptional circumstances.

**Recommendation 4.4:** The definition of ‘data subject’ should include a natural person and in some circumstances might include a deceased person.

**Recommendation 4.5:** Sensitive information should be determined depending on the context and not on listing categories of information as sensitive.

**Recommendation 4.6:** The definition of ‘data controller’ should include the natural or legal person, public authority or any other body.

**Recommendation 4.7:** The definition of ‘data processor’ should include a natural or legal person and public authority which transact personal data on behalf of data controller.

**Recommendation 4.8:** Family and personal affairs should be excluded from data protection law.

**Recommendation 4.9:** Data protection obligations should be implemented on public authority and private sectors.

**Recommendation 4.10:** Data protection law should be implemented on the processing of personal information accessed in the course of commercial and non-commercial transactions.

**Recommendation 4.11:** Data protection law should not exclude small businesses from the law’s application.

**Recommendation 4.12:** Privacy law should provide exceptions from the application of the law for reasons of defence and national security.
Recommendation 4.13: privacy law should not give any committees or ministers the power to provide new exception to the law.

Data protection law should provide strict rules regarding the procedures for dealing with personal information such as giving notice to data subjects before processing their data to other firms or organisations and also strict rules considering security principles through which each firm or organisation should provide enough steps to secure individuals’ data. The principles of privacy law should be clear enough to prevent any misunderstanding and limitations to the law. In particular the thesis recommends that:

Recommendation 4.14: data protection law should include principle which requires that personal data must be processed fairly and lawfully and shall be accurate and, where necessary, kept up-to-date.

Recommendation 4.15: data protection law should ensure that data subjects have the right to access, block and correct their personal data.

Recommendation 4.16: privacy law should require data controllers to follow the principles of purpose specification and use or collection limitation in order to ensure that data subjects are given clear protection regarding the transferring of their personal information.

Recommendation 4.17: data protection law should require data controllers to adopt opt-in formats as it will guarantee extensive protection to personal data.

Recommendation 4.18: data protection law should require data controllers to follow reasonable steps to secure data subjects information. Also, the law should adopt data breach notification requirement which requires data controllers to give data subjects notices which state that their personal data has been breached.
**Recommendation 4.19**: data protection law should commonly permit the transfer of personal information only to nations that can provide a sufficient level of data protection.

Because the enforcement mechanism of any legislation is the cornerstone for applying law effectively, data protection law should establish a Data Protection Authority because worldwide, supervisory agencies have played a critical role in monitoring the processing of personal data and considering any contravention to privacy law. The Data Protection Authority should play a vital role in educating consumers and increasing the public’s awareness regarding the protection of personal data. Data subjects should gain knowledge about their personal information rights and how to take legal action against everyone who infringes the privacy Act. In particular the thesis recommends that:

**Recommendation 5.1**: privacy law should give Data Protection Authority adequate powers in order to perform effectively.

**Recommendation 5.2**: Data Protection Authority should be given the power to hear claims concerning the protection of personal data and also investigate any breach of privacy law.

**Recommendation 5.3**: Data Protection Authorities should be required to publish reports regarding the activities conducted by the commissioner.

**Recommendation 5.4**: Data Protection Authority should have the right to provide Advice with regard to implementing the privacy law.

**Recommendation 5.5**: data protection law should give a Data Protection Commission the power to decide whether the place outside the country provides efficient personal data protection.

**Recommendation 5.6**: the commissioners of Data Protection Authority should have the power to carry out research and recommend amendments to the law.
**Recommendation 5.7:** data protection law should require the commissioners of Data Protection Authority to develop and conduct information programs to foster public understanding of the law.

Data protection commissioners should meet particular requirements regarding the process to appoint them to supervisory agency. To ensure the independence of any Data Protection Commission, it is believed that the commissioners should be chosen by following the process that is suggested in chapter five. It is important that a Data Protection Commission practice its activities free from any interference that might affect negatively their decision-making. In particular the thesis recommends that

**Recommendation 5.8:** data protection law should ensure that data protection authority meet the requirement of autonomy and transparency.

**Recommendation 5.9:** the Libyan Data Protection Commission should be established as the Supreme Commission of Applying the Required Standards for Holding Public Positions has been established.

The Libyan policy-makers should ensure that remedies and sanctions which will be enforced when personal data is breached are adequate to guarantee a real deterrent. The reason for such remedies and sanctions is that data controllers will consider them before committing any illegal activities with the processing of personal data. In addition, data subjects will have confidence in processing their data when there are severe sanctions that will be enforced against potential offenders. In particular the thesis recommends that:

**Recommendation 5.10:** privacy law should give data protection commissioners the power to use enforcement notices in order to address any infringement to the act.

**Recommendation 5.11:** the court should be given the power to enforce orders that aim to redress any offences by data controllers.
**Recommendation 5.12:** the law should ensure that any person who suffers damage when data controller infringes the law is entitled to compensation from data controller.

**Recommendation 5.13:** data protection authority might be given the power to enforce civil monetary penalty in some circumstances where there is breach to privacy law.

**Recommendation 5.14:** the law should ensure that fines are enforced on offenders who breach the law.

**Recommendation 5.15:** the law should force prison sentences on offenders who breach the law.

These recommendations are presented here to act as a guideline for the Libyan policy-makers when they consider the issue of privacy. As e-commerce grows in Libya, there will be an increasing need to address the issue of privacy; thus, data protection law should be in place as soon as possible to tackle any privacy concerns. It is obvious that personal information plays a vital role in economic growth in any State; however, this personal information should be under the data subjects’ control. The law will aim to balance between the data subjects’ interests to protect their personal information and data controllers’ interests to gain benefits from sharing personal data.
1. Hadith

Sahih Muslim, Book 7, the Book of Pilgrimage (Kitab Al-Hajj), ch 17, no 2803 a

Sahih Al-Bukhari, Hadith 6317

Sahih Al-Bukhari, Hadith No 6439

2. Books


Al Hytami, Alhafid, Majmah Alzweed and Manbaa Alfawaed (Dar Alfikr Alarabi, Beirut, 1992)


Cate, Fred H, Privacy in the Information Age (Brookings Institute Press, Washington D.C. 1997)

Fitzgerald, Brian et al, Internet and E-commerce Law, Business and Policy (Thomson Reuters, NSW 2011)


Ismail, Noriswadi and Edwin Lee Yong Cieh, Beyond Data Protection: Strategic Case Studies and Practical Guidance (Springer, 2012)


3. Journal Articles


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


Sovern, Jeff, ‘Opting in, Opting out, or No Options at All: The Fight for Control of Personal Information’ (1999) 74 Washington Law Review.


4. Newspapers


‘European data watchdogs target Google over privacy’ (2 April 2013) BBC News <http://www.bbc.co.uk/news/technology-22003551>

‘EU taskforce takes legal action against Google’ (2 April 2013) DW News <http://www.dw.de/eu-taskforce-takes-legal-action-against-google/a-16715381>


5. Treaties and Agreements

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, CETS No 181, opened for signature 8 November 2001 (entered into force 1 July 2004)


Cairo Declaration on Human Rights in Islam (Aug. 5, 1990)


EU Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature 28 January 1981, CETS No 108 (entered into force 1 October 1985)

EU-Libya Draft Framework Agreement, tit iv: Trade and Trade-related Matters (trade in services, establishment and e-commerce) Unpublished material

International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 150 (entered into force 23 March 1976)

Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, 3rd session, 183 plen mtg, UN Doc A/810 (10 December 1948)

Universal Islamic Declaration of Human Rights (19 September 1981)

6. Directives and Guidelines

The European Union (EU), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ1995 L281, p.31)
Guidelines for the Regulation of Computerized Personal Data Files, UN doc 45/95 (14 December 1990)


OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013)

7. Legislations

The Libyan Constitutional Declaration (2011)

The Libyan Penal Code (1953)

Act No 4 (1990) on the National System for Information and Documentation (Libya)

Law no 4 (2011) amends the law no 6 (2006) which organises the judiciary system (Libya)

Data Protection Act 1998 (UK)

Personal Data Protection Act 2010 (Malaysia)

Personal Information Protection and Electronic Documents Act SC 2000 (Canada)

Privacy Act1988 (Cth)

Privacy Act of 1974, 5 USC § 552a

Political and Administrative Isolation Law no 13 (2013) (Libya)

8. Cases

Gaskin v. UK (1989) 12 EHRR 36

College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer [2009] (C-553/07) European Court reports I-03889

Copland v. United Kingdom [2007] ECHR 253

European Commission v Federal Republic of Germany [2010] (C-518/07) European Court Reports I-01885

European Commission v Republic of Austria [2012] (C-614/10) European Court Reports

HALFORD v. THE UNITED KINGDOM [1997] ECHR 32

Lindqvist [2003] (C-101/01) European Court Report I-12971

MALONE v. THE UNITED KINGDOM [1984] ECHR 10

192
9. Dissertations


Corliss, Michael, The Use of Information: How New Technology is Changing Discussions of Privacy (Masters Degree, Georgetown University, 2010) <http://repository.library.georgetown.edu/bitstream/handle/10822/553697/corlissMichael.pdf?sequence=1>


10. Internet Materials and Reports


Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (t-pd), Kingdom of Morocco - request to be invited to accede to Convention 108, Council of Europe (18 October 2012) <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%2909Rev_en_opinion_Morocco.pdf>


11. Conferences


