DOCTOR OF PHILOSOPHY

The efficacy of Iraq law to deal wqith identity theft and proposals for a more legally effective solution, with comparative references to US and UK laws

Jassim, Hamdi

Award date:
2014

Awarding institution:
Bangor University

PRIFYSGOL
BANGOR
UNIVERSITY

The Efficacy of Iraq Law to Deal with Identity Theft and Proposals for a More Legally Effective Solution, with Comparative Reference to US and UK Laws

Hamdi Taih Jassim (LLB, LLM -Baghdad)

A thesis submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy

[In Law]

School of Law

College of Business, Law, Education and Social Sciences

Bangor University

May 2014

Abstract

This thesis deals with a specific type of crime, which is, today called a millennium crime. This crime is identity theft. It is not a new crime, but technological development makes it a difficult crime to combat, as nowadays it can be committed by both traditional, so-called non-sophisticated methods, and by more sophisticated, technological means, since the advent of the internet.

Identity theft is a crime committed against a person's means of identification or their financial information. The criminal, legally or illegally obtains another person's means of identification for the purpose of either himself (or others) using it to commit other illegal activities. Iraq, currently, has no dedicated law to deal with identity theft. Therefore, the Iraq courts will find it difficult when they seek to apply existing legal texts, to deal with it effectively. Through an examination of Iraqi criminal laws, this thesis will assess whether existing Iraq criminal law is adequate to combat identity theft, and it will assess whether Iraq courts can effectively judge an accused who obtains another person's means of identification, and then uses to commit other crimes. It seems that, first sight that identity theft shares common elements with theft offence in Iraq law, and thus, the Iraqi courts may use the current theft offence laws to fight identity theft, but this study will show that this has limitations and drawbacks. Comparative analysis with the relevant UK and US laws used to combat identity theft will form part of this analysis, in an effort to assess the effectiveness of this approach, and illustrate its weaknesses.

While this thesis preparation was being undertaken, the Iraqi Government proposed a project called the *Information Crimes Project 2011*. This project inter alia proposed to govern identity theft with new model laws. This thesis demonstrates that this project will not succeed in realising this objective, and the thesis shows, in conclusion, existing laws, as well as proposed laws, are inadequate to govern identity theft in Iraq, and their inadequacy requires either a judicial or legislative solution. The thesis demonstrates the limitations of judicial solution because the application of the principle of legality, and concludes that the most effectively way for Iraq to combat identity theft would be to enact a new, dedicated law to fight identity theft. To assist the Iraqi legislature to enact an appropriate piece of legislation, this thesis analyses relevant UK and US laws, and assesses

elements of those laws, and their utility for the Iraqi legislature, should it seek to borrow or adopt provisions from them for a new Iraqi identity theft law. One of the key findings of this thesis is that the actual identity theft must be criminalised, and this is something that is not a feature in laws of other jurisdictions, although there are several elements of other jurisdictions' laws which, if suitable adapted, could be useful incorporated into an Iraqi identity theft law.

This thesis concludes by proposing recommendation that will be guide the Iraqi legislature if it intends to enact a dedicated identity theft law at some point in the near future.

Declaration and Consent

Details of the Work

I hereby agree to deposit the following item in the digital repository maintained by Bangor University and/or in any other repository authorized for use by Bangor University.

Author Name: Hamdi Taih Jassim

Title: The Efficacy of Iraq Law to Deal with Identity Theft and Proposals for a more Legality Effective Solution, with Comparative Reference to US and UK Laws

Supervisor/Department: Professor Dermot Cahill/ School of Law

Funding body (if any): Iraqi Higher Education Ministry

Qualification/Degree obtained: PhD

This item is a product of my own research endeavours and is covered by the agreement below in which the item is referred to as "the Work". It is identical in content to that deposited in the Library, subject to point 4 below.

Non-exclusive Rights

Rights granted to the digital repository through this agreement are entirely non-exclusive. I am free to publish the Work in its present version or future versions elsewhere.

I agree that Bangor University may electronically store, copy or translate the Work to any approved medium or format for the purpose of future preservation and accessibility. Bangor University is not under any obligation to reproduce or display the Work in the same formats or resolutions in which it was originally deposited.

Bangor University Digital Repository

I understand that work deposited in the digital repository will be accessible to a wide variety of people and institutions, including automated agents and search engines via the World Wide Web.

I understand that once the Work is deposited, the item and its metadata may be incorporated into public access catalogues or services, national databases of electronic theses and dissertations such as the British Library's EThOS or any service provided by the National Library of Wales.

I understand that the Work may be made available via the National Library of Wales Online Electronic Theses Service under the declared terms and conditions of use (http://www.llgc.org.uk/index.php?id=4676). I agree that as part of this service the National Library of Wales may electronically store, copy or convert the Work to any approved medium or format for the purpose of future preservation and accessibility. The National Library of Wales is not under any obligation to reproduce or display the Work

in the same formats or resolutions in which it was originally deposited.

Statement 1:

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree unless as agreed by the University for approved dual awards.

Signed …….. (candidate)
Date ……..

Statement 2:

This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used, the extent and nature of the correction is clearly marked in a footnote(s).

All other sources are acknowledged by footnotes and/or a bibliography.

Signed ……. (candidate)
Date …….

Statement 3:

I hereby give consent for my thesis, if accepted, to be available for photocopying, for inter- library loan and for electronic repositories, and for the title and summary to be made available to outside organisations.

Signed ……. (candidate)
Date …….

NB: Candidates on whose behalf a bar on access has been approved by the Academic Registry should use the following version of Statement 3:

Statement 3 (bar):

I hereby give consent for my thesis, if accepted, to be available for photocopying, for inter-library loans and for electronic repositories after expiry of a bar on access.

Signed …… (candidate)
Date ……

Statement 4:

Choose **one** of the following options

a)	I agree to deposit an electronic copy of my thesis (the Work) in the Bangor University (BU) Institutional Digital Repository, the British Library ETHOS system, and/or in any other repository authorized for use by Bangor University and where necessary have gained the	
b)	I agree to deposit an electronic copy of my thesis (the Work) in the Bangor University (BU) Institutional Digital Repository, the British Library ETHOS system, and/or in any other repository authorized for use by Bangor University when the approved **bar on access** has been lifted.	
c)	I agree to submit my thesis (the Work) electronically via Bangor University's e-submission system, however I **opt-out** of the electronic deposit to the Bangor University (BU) Institutional Digital Repository, the British Library ETHOS system, and/or in any other	

Options B should only be used if a bar on access has been approved by the University.

In addition to the above I also agree to the following:

1. That I am the author or have the authority of the author(s) to make this agreement and do hereby give Bangor University the right to make available the Work in the way described above.

2. That the electronic copy of the Work deposited in the digital repository and covered by this agreement, is identical in content to the paper copy of the Work deposited in the Bangor University Library, subject to point 4 below.

3. That I have exercised reasonable care to ensure that the Work is original and, to the best of my knowledge, does not breach any laws – including those relating to defamation, libel and copyright.

4. That I have, in instances where the intellectual property of other authors or copyright holders is included in the Work, and where appropriate, gained explicit permission for the inclusion of that material in the Work, and in the electronic form of the Work as accessed through the open access digital repository, *or* that I have identified and removed that material for which adequate and appropriate permission has not been obtained and which will be inaccessible via the digital repository.

5. That Bangor University does not hold any obligation to take legal action on behalf of the Depositor, or other rights holders, in the event of a breach of intellectual property rights, or any other right, in the material deposited.

6. That I will indemnify and keep indemnified Bangor University and the National Library of Wales from and against any loss, liability, claim or damage, including without limitation any related legal fees and court costs (on a full indemnity bases), related to any breach by myself of any term of this agreement.

Signature: …… Date: ……

Table of contents

i

Dedication

I dedicate this work to my beloved parents (late) – Mr. Taih and Mrs. Aneeda, my sister (Ebtisam), and my five caring brothers.

Acknowledgements

First and final thankfulness is for my God who gives me guidance and assistance to accomplish this thesis.

I am would like to express my love and appreciation for my Prophet Mohamed صلى الله عليه وسلمwho takes me from darkness to lightness.

Secondly, I am very pleased to use this opportunity to express my indebtedness and profound gratitude to a number of individuals for their helpful guidance and assistance and other contributions throughout my study.

The first person that I thank is my supervisor Professor Dermot Cahill, to whom I am indebted for his suggestions, enlightenment, and his constant moral and material encouragement during the study, which has certainly contributed immensely to the quality of this research and which will guide me beyond this.

Sincere thanks are due to the Iraqi Ministry of Higher Education and Scientific Research for awarding the scholarship and giving me the opportunity to study at Bangor University and to complete my study.

I would like to thank all staff in both the Iraqi Department of Missions and Cultural Relations and Diyala University School of Law for financial support and their efforts in assisting me.

I would like to express my deep appreciation to my dear friends Ahmed Dhary and Muthanna Sarhan who have provided the assistance and encouragement that lifted my flagging spirit to overcome the difficulties of the study.

I am also grateful to my colleagues, especially Saud Alremethi for always being ready to listen, to discuss difficulties, and give advice.

Also, I would like to thank many British people, and students, both male and female especially my Welsh PhD colleague Huw Pritchard and Herbert Farrington for their assistance.

I am grateful for my brothers and their sons and daughters, especially the lovely daughter Baraa and her uncle Ahmed for their encouragement and their easing my difficulties and my burdens.

I owe an everlasting debt to my dear departed parents (Taih and Aneeda) who in spirit supported and encouraged me to complete my study. Although it was so difficult to continue my studies without their presence in my life, I always felt that they were with me throughout. I present my work to them with all my love that will never end.

I also express my thanks and appreciation to Iraqi Judges, prosecutors, academics, and lawyers who have responded to my questions and enquiries and during personal interviews.

I wish to extend my thanks and appreciation to Mrs. Mairwen Owen, the friendly and kindly Law Librarian, for her tireless assistance. I thank also all staff in both the Law and Deniol libraries at Bangor University for their helpful assistance when it was needed. I would like to thank my Supervisor secretary (Mrs. Anwen Evans), for her unlimited assistance and patience.

I would like to thank my wife and my father-in-law and mother-in-law for what they did.

قال الله سبحانه وتعالى: وَعَسَى أَنْ تَكْرَهُوا شَيْئًا وَهُوَ خَيْرٌ لَكُمْ وَعَسَى أَنْ تُحِبُّوا شَيْئًا وَهُوَ شَرٌّ لَكُمْ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ. البقرة 216

وقال سبحانه وتعالى: وَمَا كَانَ لِمُؤْمِنٍ وَلَا مُؤْمِنَةٍ إِذَا قَضَى اللَّهُ وَرَسُولُهُ أَمْرًا أَن يَكُونَ لَهُمُ الْخِيَرَةُ مِنْ أَمْرِهِمْ وَمَن يَعْصِ اللَّهَ وَرَسُولَهُ فَقَدْ ضَلَّ ضَلَالًا مُّبِينا. الاحزاب 36

Last, but by no means least, I owe a special debt of gratitude to my sister who has often provided moral support and encouragement, which lifted my lagging spirit. She was

always with me during the hard times I faced. My life without her would be rather difficult. I present my work to her with all my recognition and thankfulness for everything.

Finally, my apologies to those of you reading this and other who have contributed, who I have forgotten to mention, but please accept my sincere thanks. Thanks to everyone.

شكرا جزيلا!

Acronyms/Abbreviations

USA, US= United States
UK= United Kingdom
IT= Identity theft

ID= Identification

ATM= Automated Teller Machine

SSN= Social security number

PIN= Personal identification number

FBI= Federal Bureau of Investigation

Introduction

The aim of this study is to assist the Iraqi legislature to define identity theft and a proper legal framework to fight it because Iraq has no specific law to fight this type of crime. For the reasons given below, the legal fight against identity theft has become more urgent recently.

Identity theft can be defined as the obtaining of, or transferring of, another person's means of identification, and then using it to carry out others crimes, such as fraud, avoiding arrest by the police or carrying out terrorist operations. The main motive of stealing one or more than one of another person's means of identification is to use it to commit fraudulent activities, such as stealing money. Identity theft has become a common economic crime in major economies, such as US,[1] and now proliferating to less developed economies like Iraq. It is called a white collar crime. It is also called a crime of the information age.

It is not a new crime; however, technological development makes it a fast growing crime around the world. Impacts that are caused by crimes committed by using stolen identity is becoming a serious social issue, affecting millions of people and organisations every year.[2] It poses a complex problem, spans the borders of many organisations, companies, and countries. It may affect numerous entities in different methods and at different times.

Identity theft is a crime that is committed against a person's means of identification. This means of identification has a specific nature. It is intangible. As a result, to get this information, the criminal uses methods that differ from those that are used to commit traditional crimes of theft. Identity theft can be committed by using two methods: traditional methods, such as searching in trash, stealing an individual's wallet or purse, or shoulder spoofing; and non-traditional or sophisticated methods, such as phishing, malware, or Trojan Horse.

---

[1] Susan E Bernstein, 'New Privacy Concern for Employee Benefit Plans: Combating Identity Theft' (2004) Vol.36 (1) Compensation and Benefits Review 65-68; M W Perl, 'It's not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft' (2003-2004) Vo. 94 (1) the Journal of Criminal Law & Criminology 169-208.

[2] M W Perl ibid

Methods that are used to commit identity theft can be divided into two types: offline methods and online methods. It is difficult to prevent, discover or detect offline identity theft,[3] because its discovery depends on having constant vigilance over documents containing identity information that may be issued by institutions that the victim deals with, such as a bank. Due to advances in technology and the advent of the internet, which has become the lifeblood of many commercial transactions, more and more transections are being conducted online with greater ease and efficiency. Often, these transactions require an exchange of personal information between customers, businesses, government agencies, and financial institutions. The internet has erased economic borders and further strengthened the concept of global communication. Consequently, individuals' information becomes widely distributed.[4] For the purpose of this thesis, an individual's information or means of identification encompasses both the person's means of identification and his financial information.

More and more countries are joining the global networked economy. Iraq is one of those countries. People use the internet to accomplish their transactions, which cannot be achieved unless by spending much time and money. The use of the internet to accomplish transactions makes a person's information available widely because the internet has no administrative borders. This pervasiveness of the individuals' information on the internet and the vulnerabilities that may be found on the internet makes this information an attractive and easy target that can be obtained by people with criminal intent without the owner's knowledge.[5] Identity thieves around the world are constantly seeking loopholes by which they can obtain a person's means of identification. Moreover, the internet allows some perpetrators to commit identity theft remotely. It also gives them the ability to conceal their crimes. As a result, committing

[3] People sometimes do not know that they have become a victim of identity theft, or they know this, but after a long time. Even if they know that they have become a victim, they may find it difficult to discover and detect the perpetrators. The law enforcement officials may also find it difficult to discover the crime or to prove that the perpetrator is guilty of identity theft.

[4] K Zaidi, 'Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguards Personal Data in the United States and Canada' (2007) Vo. 19 (2) Loyal Consumer Law Review 99-150

[5] In *building of* Presidency Federal *Appeals Court Basra, Basra's judges have held a conference to discuss the electronic crime and its effects on people and government. At the end of the conference, they stated in their conclusion that* the Iraqi legislature should enact new legislation to curb this type of crime. They have also stated that this type of crime is considered a dangerous crime. It may be used by organised criminals to commit an organised crime. Therefore, they have requested the legislator to enact new legislation to curb it, SKM, 'Judges of Basra Request Enacting Legislation to Curb Electronic Crime and they warn from using it within the Scope of Organized Crime'. ALMada Press, available at <http://www.almadapress.com/ar/news/11496/> accessed on 21 June 2013

online identity theft has become easy. Achieving transactions online and facelessly encourages unscrupulous persons to obtain a person's means of identification a variety of ways either on or offline.

To fight identity theft, and to mitigate the above risks of identity theft, and to protect people's identities, the Iraqi legislature should enact a specific law to curb identity theft, because Iraq still has no specific law to serve that end. Consequently, courts have to apply existing laws to fight identity theft. One type of current laws that may be applied to identity theft is theft offence laws. However, due to the specific nature of the personal and financial information the subject of identity theft, some difficulties may arise and confront courts when they attempt to apply the current Iraqi theft offence laws to a person who obtains another person's means of identification without consent, and then uses it to commit other illegal activities.

These difficulties can be formulated through three questions that will be examined in this thesis: is a person's means of identification considered property according to the definition of property that is stipulated in theft offence laws? Can it be subject to physical seizure? Finally, is the person permanently deprived of his means of identification? To overcome the above challenges Iraqi courts may attempt to interpret extensively the current theft offence laws (or create new laws) to govern identity theft, failing this, the Iraqi legislature should enact a new law to cover it.

Two outcomes may appear as a result of the above analysis of current Iraqi theft offence laws: either the courts can apply these laws to combat identity theft, or these above difficulties remain unresolved and the courts cannot apply the current theft offence laws to govern identity theft. In the event of the latter outcome, the question will arise whether the criminal judge can overcome the legislative inadequacy by extending the current theft offence laws (or by creating new laws) to govern identity theft.

By analysing these issues, the author has realised that challenges have been triggered and found and that existing Iraqi theft laws prove ineffective and inadequate to cover identity theft. He has also realised that Iraqi judges cannot overcome these challenges by extending the current theft offence laws (or by creating new laws). The study also shows that the Iraq Information Crimes Project 2011 is inadequate to govern identity

theft.

To overcome the legislative and judicial inadequacy the thesis has attempted to examine whether the Iraqi legislature can adopt or borrow provisions from either US, or UK legislation, or from both to enact a comprehensive identity theft law for Iraq. The study shows that the Iraqi legislature could borrow or adopt provisions from the UK legislation to amend the fraud offence law or enact a new Act to fight computers misuse, but reliance on UK laws will not be sufficient to criminalise the actual theft of identity *per se*. With respect to the analysis of US identity theft laws, the study also shows that while the Iraqi legislature could borrow or adopt provisions from the US identity theft laws, it must ensure that it avoids some of the flaws identified in the US legislation. Finally, the author provides recommendations, which may be helpful to the Iraqi legislature when it comes to enact an identity theft offence law for Iraq.

Chapter One

Background of the Topic of Thesis

Introduction

In this chapter, the author attempts to give a flavour of the background to identity theft, and illustrate some issues, such as the misnomer of the term identity theft to refer to the illegal obtaining of people's identities; background about identity theft as a crime; the importance of the thesis topic for Iraq, literature review; reasons for choosing this topic as a PhD thesis; thesis statement; structure of thesis; and methodology. Due to the US is considered the country most susceptible to identity theft, and it has significant experience and specific laws to deal with identity theft, numerous examples relating to identity theft that are given in this thesis will be taken from the US jurisdiction[1] to illustrate the sophisticated nature of identity theft.

1. Misnomer to Use the Term of Identity Theft

Some scholars, professionals, and jurisdictions whether in Iraq or not, brand the use of or transfer of another person's means of identification as identity theft. In effect, the use of, or transfer of another person's means of identification is a stage that comes after the commission of the actual identity theft. As it will be shown in the next section, identity theft has occurred as a crime, completed once the *actus reus* (the taking of identity) is completed.

1.1 A Continuing Crime and the Temporary Crime and Identity Theft

A crime is an act that is committed by a person, causes a social violation or disorder

[1] Unlike to the United States, Iraq has no specific law to deal with identity theft. Consequently, there is no clear definition for this crime in the Iraqi and other Arab countries legislation. Theft offence laws that are in place have been enacted before the act of the unlawful obtaining of people's means of identification and then using it to commit crimes has become an issue. The current Iraqi theft offence laws have remained static to protect tangible property while intangible things (individuals' information has become more susceptible to theft) are not covered. Theft of people's information was beyond what the Iraqi legislature of theft offence laws could have envisaged at the time of enacting these laws.

whether it is public or specific and it is punishable by the law.[2] According to Arab and Iraqi scholars' literature, the crime is divided into many types according to its *actus reus*, such as a positive crime and negative crime,[3] a temporary crime and a frequent crime,[4] a simple crime and habitual crime[5] and a continuing crime and a temporary crime. Insofar as to relate the above types of the crime to the crime that is distinguished in this thesis, the types of continuing and temporary crime will be discussed below.

1.1.1 Temporary and Continuing Crime

Temporary and continuing crimes are two different types of crime. Each of these types will be discussed below.

1.1.1.1 A Continuing Crime

A continuing crime consists of an act that requires a frequent intervention of the will of the criminal,[6] such as possessing a weapon without licence, the mother's failure to breast-feed her baby or opening a public shop without getting permission from the authorities. The *actus reus* of this type of crime is recommitted each time the criminal intends to commit it without achieving that required conditions to use it. For instance, a person is guilty of possession of a weapon without licence each time he uses this weapon without getting a licence.

The continuing crime gives rise to many issues, such as the jurisdiction of the judge and the application of the law to this crime. For example, the commission of the continuing

---

[2] A Qaisi, 'Crimes Dividing According to the *Actus Reus*' available at <http://www.lawjo.net/vb/showthread.php?t=11879> viewed on 28 August 2011

[3] A positive crime is a crime, which needs a physical movement from the criminal to occur, such as theft, forgery, and fraud while a negative crime means a crime, which occurs as a result to the failure of the criminal from doing a legal duty assumed by the law. A Qaisi, ibid

[4] A frequent crime is a crime consists of series acts lead to one or the same result, such as theft from the same person, but in different times and the electric power theft while a temporary crime is a crime consists of one act or many acts, which occur and finish at the same time, such as theft, murder and fraud. M Alraezki, *Lecturers in Criminal Law, General Part, General Principles, a Crime and Responsibility*, (3rd edn, Dar Oya 2002) 68-72, A frequently crime requires three conditions; these acts should be similar and aim to the same result; it should occur against the same victim; and the time between the first act and other act(s) should be short. A Qaisi, supra, note 2

[5] A simple crime is a crime consists of act or more than one act that the law does not require repeated it such as theft, murder, fraud and forgery while a habitual crime is a crime that the law requires repeated the act that constitutes the crime to consider it as a punishable crime, such as acquiring a prostitute or drinking alcohol. A Qaisi, supra, note 2; M Alraezki, ibid 96

[6] M Alraezki, supra, note 4, 68-69

crime may start in a place that relates to the authority of a judge, and then it may be completed in other places that relate to the authority of another judge. In addition, it may be subject to a new Act, which may be stricter than the previous law. In these cases, every judge under whose authority the continuing crime is committed can rule against the accused who commits it. More so, due to the continuing crime consisting of a series of acts, it may be governed by an existing Act when it is discovered regardless of whether it was strict or not. Moreover, the continuing crime renews every time that the criminal commits the *actus reus* of it. The *mens rea* of this crime is the criminal intention to commit the *actus reus* of this type of crime continually.[7]

1.1.1.2 A Temporary Crime

A temporary crime or an instant crime consists of an act that takes place and finishes at the same time,[8] such as theft and murder. Implications of a crime do not affect the nature of the crime. The crime is still described as a temporary crime, whether or not its implications continue for a long, or short time. For instance, if the person steals a car of another person the theft offence is completely performed by taking the car away and permanently depriving the owner of it. However, the use of the car for the criminal benefit, such as selling or giving it to another does not refer to theft; it is called an implication of theft. The result in this type of crimes immediately occurs when the *actus reus* is complete.

1.1.2 Distinguishing Between a Temporary Crime and Continuing Crime

The nature of the *actus reus* of the crime as it is defined in the criminal law is considered the main factor to distinguish between a temporary crime and a continuing crime whether of the nature of the *actus reus* is positive or negative or whether it has been committed intentionally or neglectfully. For instance, a crime, such as theft, is considered a temporary crime if it is started and finished merely when the *actus reus* occurs while a crime, such as possessing heroin is considered a continuing crime because it continues as long as the *actus reus* continues.[9] Time is more important in

[7] W Haddad, 'If You Wants to Be a Unique Lawyer You Should Know These Crimes' 2008 available at <http://pbapls.3arabiyate.net/t41-topic> viewed on 27 August 2011
[8] M Alraezki, supra, note 4, 68
[9] W Haddad, supra, note 7

distinguishing between a temporary and a continuing crime. For example, the crime is considered a temporary crime if the result of it immediately or after a period of time occurs and is not interfered with the will of the criminal again. However, it is considered a continuing crime if the result of it does not immediately take place and it needs to interference from the will of the criminal to be completed.[10]

1.1.3 A Common Misnomer

In Iraq, scholars have written about technology crimes, but they have not written about identity theft. Sometimes in their literature, they refer to an identity theft crime as an example of technology crimes. However, in other countries, many authors whether specialists or not, have written about identity theft as a crime. The author has observed that most of them have no idea about the elements of it or ignore these elements. In addition, they have no idea about types of crimes as have previously been illustrated. Consequently, they are confused between identity theft and its implications. Identity theft may be defined as the illegal obtaining of the personal or financial information of another person, and then using it for gain or committing other crimes.[11] It is also defined in the section 1028 of the Identity Theft and Assumption Deterrence Act 1998 US as:

> (a) Whoever, in a circumstance described in subsection (c) of this section: 7. knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.[12]

As will be shown, according to the concept of crime, identity theft consists of two main elements *actus reus* and *mens rea* and a third element a means of identification is referred as to the subject of crime. (1) the *actus reus* contains the traditional and sophisticated methods that are used to commit identity theft, the use of or transferring of another person's means of identification; (2) *mens rea* that represents the criminal state of mind and (3) the subject matter of crime 'an individual's means of identification'.

---

[10] A Qaisi, supra, note 2

[11] M D White, 'Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts' (2008) Vol. 19 (1) Criminal Justice Policy Review 3-24

[12] Identity Theft and Assumption Deterrence Act 1998, Pub. L. 105-318, 18 §1028 Sec. 3 (a) (7) October 30, 1998, 112 stat. 3007

Identity theft is considered a temporary crime because it starts and finishes at the same time that the *actus reus* of it is complete. For instance, if a person steals the contents of mailbox with intent to take personal financial information of another person that may be found with these contents he may be guilty of identity theft because the elements of identity theft have completed when the person takes the information. Actions that are committed after that, such as the use of this information to commit other crimes are not considered parts of the *actus reus*. These actions are considered implications of identity theft. Furthermore, these implications may constitute separated crimes, such as fraud, terrorism or the evasion from another crime.

More so, even if the criminal bribes a worker or officer in an office to steal information from his/her employer, bank, or company, he may not be guilty of identity theft because he does not commit the *actus reus* of identity theft. He may be guilty of using stolen identity to commit other crimes if he uses it to commit other crimes or he is a secondary participant in identity theft. The principal actor of identity theft in this case is the worker or the officer who steals the information. The use of stolen identity is considered a preparatory act or a means to commit other crimes. As a result, every act that is committed after taking another person's information by one of the methods that will be discussed later, does not amount to identity theft. However, it may be considered to be another crime that is also committed by using stolen identity. Below is literature review that may explain scholars' perspectives about identity theft.

1.1.4 Literature Review

Identity theft is an old crime, but it has a new fashion. It is considered a millennium phenomenon. It has the fastest growing rate in the world. It has many effects on all parties, such as states, companies, and individuals, thus there is no one immune from this crime.[13] For example, it may target all individuals, in all their ranks, or their ages. It does not distinguish between a person of high rank or an ordinary citizen, an adult or a child, alive or deceased, an academic person or not.

In addition, identity theft costs states billions of dollars every year. For instance, according to a statistic in the United States, the number of identity theft victims was

[13] D M Ingram, 'How to Minimize Your Risk of Identity Theft' (2006) Vol. 77 (6) Optometry, Journal of the American Optometric Association 312-314

approximately 100,000 per year, and the cost was $2 billion per year,[14] as well, it costs the United Kingdom £16.1m per year.[15] Individuals who are a victim of identity theft suffer from two types of damages: financial and emotional damages. Victims may lose their money if the criminal uses their information to open a new account or perpetuate an existing account. In addition, they may spend much time to repair their credit history. Furthermore, their reputation may be wrecked when their identities have been used by criminals.

In this literature, scholars and professionals' perspectives about the definition of identity theft will be illustrated. In addition, the literature will examine how identity theft takes place. It will also illustrate identity thieves and their relationship with victims. Moreover, it examines measures that may be taken by some states, such as United Kingdom and United States to protect their citizens from this epidemic crime. Most scholars, legislatures, and even laypersons believe that identity theft is a crime in itself.

According to general rule that determines a crime, identity theft consists of two main elements, *actus reus* and *mens rea*. Neither the scholars in their literature nor the legislatures in their legislation state and determine these two elements of identity theft.

Currently, criminals use sophisticated methods to commit identity theft, consequently, States and their law enforcement officials find it more difficult to discover or detect and catch them. As a result, identity theft related to cyberspace has been considered a more complex crime. It has become more complex because criminals can easily conceal their unlawful activities. In addition, they commit it from a far distance that may be out of the law enforcements' jurisdiction. Committing identity theft remotely may raise the jurisdiction problem which delays obtaining evidences on crime or catching the criminals. Moreover, it may raise an extradition or a prosecution problem. Thus, the states should cooperate with each other to combat identity theft. To illustrate the above issues the author has done a literature review about what the authors have written in this

[14] L M LoPucki, 'Human Identification Theory and the Identity Theft Problem' (2001) Vol. 80, Taxes Law Review 89-134

[15] Edgar A Whitley and Ian R Hosein, 'Policy Engagement as Rigourous and Relevant Information Systems Research: The Case of the LSE Identity Project' 2007 London School of Economics and Political Science 1301-1312 available at <http://personal.lse.ac.uk/whitley/allpubs/ecis2007.pdf> accessed on 15 February 2011

area, as well as what legislatures in different jurisdictions enacted to prevent this type of crime and protect their people.

1.1.4.1 Definition of Identity Theft

McCutcheon defines identity theft as 'the illegal use of another's personal identification numbers'[16] (such as his driver licence, date of birth or social security number). Heller also defines identity theft as 'a crime in which an imposter obtains a key piece of personal identifying information'.[17] Sproule and Archer, before defining identity theft, have stated that the term of identity theft is widespread and a better term that may be used to describe the act of the unlawful use of people's identities is identification fraud. However, they defined identity theft through defining its term because identity theft consists of two terms: identity and theft.[18] The main point that they triggered in their literature is that the use of people's identities is not crime. They conclude that the individuals' identity cannot be subject of theft because the criminal does not deprive the owner of his property. They stated that there is permission especially if theft takes place inside the work or between families.[19] Many scholars have defined identity theft, and the author highlights some of the literature in these pages and more throughout the thesis. Legislatures in other jurisdictions elsewhere in the world have also defined identity theft. For instance, in the section 1028 of the Identity Theft and Assumption Deterrence Act of 1998 US, the US legislature has defined identity theft as:

> (a) Whoever, in a circumstance described in subsection (c) of this section: 7. knowingly transfers or uses, without lawful authority, a means of identification of another person with intent to commit, or to aid or abet, any

[16] M C McCutcheon, 'Identity Theft, Computer Fraud and 18 U.S.C § 1030(g): A Guide to Obtaining Jurisdiction in the United States for a Civil Suit against a Foreign National Defendant' (2001) Vol. 13 (1) Loyola Law Review 48

[17] I Heller, 'How the Internet Has Expanded the Threat of Financial Identity Theft, and What Congress Can Do to Fix the Problem' (2008) Vol. XVII: 1Kansas Journal of Law & Public Policy 83-107

[18] S Sproule and N Archer, 'Defining Identity Theft- A Discussion Paper' 2006, 4 available at <http://www.business.mcmaster.ca/idtdefition/IDTDiscussionPaperRevisionfromSueSprouleApril606.pdf > accessed on 5 March 2011

[19] ibid

unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.[20]

In view of some scholars and US courts, this definition may be the best definition; however, some authors, such as Meulen; Sproule and Archer; Newman and McNally considered it too broad,[21] because it encompasses some activities that are considered merely preparatory activities. In contrast to the USA legislature, the Canadian legislature defines identity theft in the s4 of the Canadian Bill 2009, which amended the existing Criminal Code (identity theft and related misconduct). In this section, it stated that identity theft is knowingly obtaining or possessing 'another person's identity information in circumstances giving rise to a reasonable inferences that the information is intended to be used to commit an indictable offence that includes fraud, deceit, or falsehood as an element of the offence'.[22] The author suggests that the definition that is stated in the Criminal Code of Canada is adequate to govern identity theft because the Canadian legislature criminalises the act of the unlawful obtaining of peoples, whereas the US legislature does not criminalise it.

In the Theft Act of 1968, the UK legislature does not consider the act of the unlawful obtaining of another person's means of identification as a separate crime.[23] Therefore, it does not define identity theft. However, the Home Office of United Kingdom has defined identity theft as an activity, which "occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead.[24] The individuals' information that may be the stolen subject encompasses any sensitive information (such as password, social security number, mother's maiden name, address, date of birth, or credit card number).

---

[20] The Identity Theft and Assumption Deterrence Act of 1998 US, supra, note 12

[21] N Meulen, 'The Challenge of Countering Identity Theft: Recent Developments in the U.S., the U.K and the E.U, International Victimology Institute Tilburg' September, (2006) 2 available at <http://www.samentegencybercrime.nl/UserFiles/Rapportidentiteistfraudeuniversiteittilburg.pdf> accessed on 16 Feb. 11; S Sproule and N Archer, supra note 18, 6; G Newman and M McNally 'Identity Theft Literature Review' (2005) 5 available at <http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf > accessed on 6 March 2011

[22] Bill s 4 Act amended Identity Theft and Related Misconduct 404, 2(1) Canada 2009 available at <http://www.cba.ca/contents/files/submissions/sub_20090603_01_en.pdf> accessed on 25 May 2011

[23] S (1) Theft Act of 1968 c. 60 (UK)

[24] United Kingdom Home Office (2006a), 'Identity Crime Definitions' available at <http://www.identity-theft.org.uk/definition.html> accessed on 16 February 2011

It might be said that it is difficult to get an adequate definition of identity theft because the term is broad and every author looks at the crime from his perspective. Thus, identity theft may be defined as using or attempt to use dishonestly another person's name or any other identifier without the owner's consent to achieve illegal purposes or aiding and abetting in committing illegal purposes, such as committing credit card fraud or opening a new account in the victim's name.

1.1.4.2 Difference between Identity Theft and Other Crimes

There are many differences between identity theft and other crimes, such as identity fraud and identity crimes, which are committed by using people's identities. For instance, Cavoukian believes that identity theft differs from identity fraud, by the definition because identity theft means getting key pieces of someone's information in order to impersonate him and carry out different crimes in his name, while identity fraud is a crime that takes place when a person obtains an individual's property by cheating.[25] Other scholars, such as Lacey and Cuganesan believe that identity theft takes place when the person falsely represents himself as another actual person for some illegal actions, while identity fraud takes place by using either actual individual identity or using untrue identity to obtain illegal purposes.[26] In other words, as Wilcox et al[27] pointed out that identity fraud is broader than identity theft. Accordingly, Newman and Clark consider identity theft a subcategory of identity fraud.[28] With respect to the difference between the identity crime and identity theft, some scholars[29] stated that the identity crime is broader than identity theft. Sometimes identity crime contains both identity fraud and identity theft, particularly when identity theft occurs using the internet.

---

[25] A Cavoukian, 'Identity Theft: Who's Use Your Name? Information and Privacy' 1997 Commissioner/ Ontario, available at <http://www.ipc.on.ca/images/resources/idtheft-e.pdf> accessed on 16 Feb. 11

[26] D Lacey and S Cuganesan, 'the Role of Organizations in Identity Theft Response: Organization-individuals Dynamic' (2004) Vol. 38 (2) The Journal of Consumer Affair 244-261

[27] Gordon, G.R.N.A, Wilcox, et al, 'Identity Fraud: A Critical National and Global Threat' (2004)Vo. 2 (1) Journal of Economic Crime Management 7

[28] G Newman and R Clarke, *Superhighway Robbery: Preventing E-Commerce Crime* (Willan, London 2003)

[29] S Sproule. and N Archer, supra, note 18

1.1.4.3 Types of Identity Theft

Types of identity theft or the use of individuals' information after stealing it, as many scholars, such as Ingram and Hoofing call it, may take many forms (such as, financial identity theft, criminal identity theft and organisation of identity theft). Financial identity theft takes place when the criminal steals another person's information to obtain financial benefit, such as a loan or renting an apartment for himself or for another person.[30] Criminal identity theft occurs if the criminal uses another person's identifiers to avoid arrest by police.[31] Organisation identity theft takes place when more than one person makes an agreement to commit identity theft.[32] For example, if some persons agree to commit identity theft, one of them provides the laptop so that a bogus email will be sent by it, another person may design the email, or the false website and other persons receive the information that may be sent to the bogus website and then use it to commit other crime.

1.1.4.4 Identity Theft Parties

There are few researches related to the parties of identity theft. Those parties of identity theft may be the victims of identity theft or the criminals of identity theft.

1.1.4.4.1 Victims of Identity Theft

Some authors have written about victims of identity theft and about how the law can help them repair their credit card history and reputation. Drake[33] points out that the victims of identity theft encompass both individuals whose means of identification has been stolen and the companies whose information or services are stolen. Newman and McNally[34] pointed out that those victims of identity theft are the minimum and may

[30] Ch Hoofing, 'Identity Theft: Making the Known Unknowns Known' (2007) Vol.21 (1) Harvard Journal of Law & Technology14
[31] G Newman and M McNally, supra note 21, 5
[32] ibid 5
[33] E Drake, *50 Plus One Tips to Preventing Identity Theft* (Encouragement Press L L C 1261 W Glenlake Chicago IL 60660, 2006)
[34] G Newman and M McNally, supra, note 21

find other victims. Two studies indicate that there are more than 7 million victims every year in the U.S.[35]

Criminals of identity theft do not distinguish between an adult victim or a child, an old man or a young, an ordinary person or a high- ranking person. Even the deceased persons are victims of identity theft.[36] In addition, companies and financial institutions have been victims of identity theft either indirectly or directly when their information is stolen.[37]

Newman and McNally[38] stated that victims of identity theft suffer from two types of damages, physical and financial. Courts and law enforcements face many difficulties to help the victim of identity theft because identity theft sometimes committed remotely via internet and may be a subject of another jurisdiction. In addition, the police do not respond to identity theft because they believe that individuals, however, are not the true victim of identity theft, banks are the true victim.

1.1.4.4.2 Criminals of Identity Theft

Hughes[39] believes that criminals of identity theft differ from other criminals. Therefore, he describes them as opportunists because they exploit the opportunity to commit their crime. He also stated that some criminals may exploit the relationship between themselves and the victim to commit identity theft. The criminals may be the victims' friends, their parents, or children. In addition, they may violate the trust afforded to them by the victim and steal his information. This type of identity theft takes place

---

[35] E Drake, supra, note 33

[36] T L O'Brien, 'Identity Theft Is Epidemic, Can Be Stopped' New York, Times (2004, 4 October) section 3:1, 4 available at <http://www.nytimes.com/2004/10/24/business/yourmoney/24theft.html> accessed on 21 Feb. 11; G Newman and M McNally, supra note 21; 'The President's Identity Theft Task Force, Combating Identity Theft a Strategic Plan' April 2007 available at <http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/downloadabledocuments/combating_identity_theft_a_strategic_plan.pdf> viewed on 17 February 2011; D Teague, 'Authorities: Scam Took Ids of Deceased' (2004) MISNBC available at <http://www.msnbc.msn.com/id/3899283/ns/night_news/> viewed on 17 Feb. 11

[37] G Newman and M McNally, supra note 21

[38] ibid

[39] K Hughes, 'Final Report of Cognitive Research on the New Identity Theft Questions for the 2004 National Crime Victimization Survey' Studies Series Survey Methodology =2004-02, Statistical Research Division U.S Bureau of the Census Washington D.C. 20233 available at <http://www.census.gov/srd/papers/pdf/ssm2004-02.pdf> 17 accessed on 17 Feb. 11

inside the workplace, home, and among friends. Allison[40] in his article that is named "[a]case study of identity theft, 2003" stated that information and researches about criminals of identity theft are limited.

1.1.4.5 Attempt, Participation, and Conspiracy to Commit Identity Theft

Newman and McNally[41] mentioned that there are few researches on these types of activities. They pointed out that acts or behaviours by other persons to assist, abet, or agree with the criminal to commit identity theft are considered more dangerous than the identity theft. They stated that these activities might increase the commission of identity theft, especially if the criminals use the internet to commit their crime. Owing to the criminal sometimes commits identity theft from far distances requires assistance from other persons. There are many factors related to the commission of identity theft. The criminal could not carry out these factors unless other persons assist him. However, legislators and scholars in their literature do not give the attempt, participation, and conspiracy in identity theft their attention and leave them to common rules, though there are many cases involving conspiracies or participation in identity theft.

1.1.4.6 Factors That Contribute to Identity Theft Occurrence

As stated previously, there are many factors that relate to the commission of identity theft. Many scholars and professionals have discussed these factors. One of these factors is the internet, which may play a more important role to facilitate the commission of identity theft because some criminals use the internet to commit identity theft through phishing, or spam. Hoar[42] believes that the internet has created identity theft. However, other scholars, such as McCutcheon and Jennifer[43] believe that the internet does not create identity theft. It may facilitate the commission of identity theft, but not create it *per se* because identity theft was present before the invention of the internet when low technology was used by criminals to commit their crimes.

---

[40] S F. H.Allison, 'Case Study of Identity Theft' 2003 available at <http://etd.fcla.edu/SF/SFE0000093/MasterThesis.pdf> 22 accessed on 5 March 2011

[41] G Newman and McNally, supra note 21

[42] B Hoar, 'Identity theft: The Crime of the New Millennium' USA Bulletin (March 2001) Vol. 49 (2) US Department of Justice 1 available at <http://www.justice.gov/criminal/cybercrime/usamarch2001_3.htm> accessed on 17 Feb. 11

[43] M C McCutcheon, supra note 16; L Jennifer, 'Identity Theft, in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attack' (2005) Vol. 20 Berkeley Law Journal 259-299

Inadequate education is also a factor that may contribute to the commission of identity theft. Individuals should enlighten themselves about identity theft, such as how it can be committed; the ways that may be used to commit it and how they can protect themselves from it. The time that has been taken to discover identity theft is another factor that may facilitate identity theft occurrence. Many victims, for instance, do not know that they were victims of identity theft until after a long time. In addition, Chawki and Abdel Wahab[44] stated that the ability, which the criminals have to commit identity theft or to conceal their crimes and the exploitation of the relationship between the criminals and the victim, might increase the commission of identity theft. These factors may make it difficult to discover identity theft. Consequently, the law enforcement bodies find it difficult to detect the criminal of identity theft.

1.1.4.7 Methods by Which Identity Theft Can Be Committed

Ingram[45] stated that most authors in their literature pointed out that identity theft takes place either online or off line. Criminals can use many methods, such as phishing, spam, social engineering stealing wallets, mailbox theft, and malicious malware programs to commit identity theft. Stuhlmiller[46] calls these methods sophisticated and unsophisticated methods. Some states, such as UK, have enacted laws, such as the Computer Misuse Act 1990, to curb some of these methods. Some of these laws do not directly criminalise these methods; however, they indirectly curb it.

1.1.4.8 Preventing Identity Theft

Like other authors, Meulen[47] pointed out that identity theft is a serious crime, and has the fastest growing rate. In addition, it may affect all individuals, and on all levels. As stated previously, it costs the states billions of dollars every year. Therefore, most believe that it should be combated. As a result, many academic and non-academic authors, organisations, individuals, media and the states try to do what they can do to

[44] M Chawki and M Abdel Wahab, 'Identity Theft in Cyberspace; Issues and Solutions, Lex Electronica' 2006 Vol.11, N.1 (printemps, Spring, 2006) 10; J D Newton, 'Organised 'Plastic' Counterfeiting' London: Home Office, 1994 in Newman and McNally, supra note 21,5

[45] D M Ingram, supra, note 13

[46] N J. Stuhlmiller, 'Flores-Figueroa and the Search for Plain Meaning in Identity Theft Law' (2010) Vol. 58 Buffalo Law Review 221-266

[47] N Van der Meulen, supra, note 21

prevent identity theft. However, some financial institutes or other organisations do not take serious measures to prevent identity theft.

Jennifer and other scholars[48] suggested that three categories should work together to prevent identity theft. The first category is self-protection. In this way, individuals should learn and know everything about identity theft, such as how and when it can take place. They should dispose of any unnecessary documents. They mentioned also that the state should assist individuals to protect themselves. It should provide websites to disseminate news or information about identity theft. According to Jennifer's opinion, the second category is measures that may be taken by some private parties, such as financial institutions, merchants, and companies. He also stated that these institutions should take some measures to protect their clients. In the same vein, Wales[49] mentioned that companies could cooperate with a state to prevent identity theft by taking some measures, such as firewalls to prevent unauthorised access to their systems. In addition, Sprague and Ciochetti[50] argue that if these companies do not take voluntary measures to protect individuals' information, mandatory measures may be imposed on them to do so.

Turn to the opinion of Jennifer, the third category that can be used to combat identity theft is the state's efforts. Therefore, states (such as United States and United Kingdom) should enact laws to prevent identity theft. Jennifer and other authors discussed the United States laws that have been enacted to combat identity theft, such as the Fair Credit Transaction Act of 2003 that gave the Trade Commission the authority to receive victims' complaints about identity theft. Fair Credit Transaction Act obliged the credit bureaus to put a freeze on consumer's account when he presents the police with a report about identity theft. Moreover, it obliged report agencies to provide the costumers every month with reports about any changes that may have happened in their account. In

[48] L Jennifer, supra note 43; Linda and J Foley Exec. Directors, 'Identity Theft Aftermath 2003 (Identity Theft Resource Center, A Comprehensive Study – to Understand the Impact of Identity Theft on Known Victims as well as Recommendations for Reform 2003)' 1-58 available at <http://www.idtheftcenter.org/vg120.shtml> accessed on 17 March 2011

[49] E Wales, 'Identity Theft' (2003) Vol. 2003 (2) Computer Fraud & Security 5-7; N Dunne, 'ID Theft for Beginners' (2008) Vol. 2008 (1) Network Security10-13

[50] R Sprague and C Ciocchetti, 'Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws' (2009) Vol. 19 (1) Albuquerque Law Journal Science& Technology 130; see also L Jennifer, supra, note 43

addition, the United States made identity theft a federal crime through enacting a new Act, which is called the Identity Theft and Assumption Deterrence Act of 1998. As mentioned previously, identity theft is a serious crime and it is difficult to be encountered. Consequently, United States enacted the Identity Theft Penalty Enhanced Act of 2004 to support the former Act to prevent identity theft. This law raised the penalty to two years for the criminal who commit identity theft by using stolen identity and five years for the criminal who uses stolen identity to commit terrorist crimes.[51]

All the above issues have been stated by Jennifer who also said that the criminal might be prosecuted by criminal laws, such as laws against card fraud, wire fraud and bank fraud.[52] However, Jennifer believed that all these efforts might not prevent identity theft because the law alone cannot prevent identity theft. As a result, all parties should cooperate with each other to combat identity theft. The law also should make some organisations or financial institutions liable[53] for any violation of individuals' privacy or giving individuals' information to another person without their consent or their knowledge. Contrary to Jennifer's opinion, Katyal[54] believes that increasing penalties may be enough to prevent identity theft, particularly if there is a correct detection of identity thieves and many of them are caught.

As pointed out previously, the Theft Act of 1968 does not consider the act of the unlawful obtaining of another person's information and then using it to commit other crimes as a crime.[55] Therefore, Meulen[56] describes United Kingdom a defenceless state because it lacks an Act that defines identity theft as a crime. However, United Kingdom Home Office has considered identity theft as a crime when it, in recent years, has noticed an increase in the crimes that are committed by using stolen identity in United Kingdom.[57] As a result of the lack of provisions in UK's laws that may be used to combat identity theft, Meulen mentioned that the UK government increased its

[51] Public Law No. 108-275, § 2, 118,Stat. 831
[52] Jennifer, supra note 43
[53] C J Hoofnagle, 'Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors' (2005) Stanford University Press 5 available at <http://papers.ssrn.co/sol3/papers.cfm?abstract_id=650162> accessed on 18 Feb. 11
[54] N K Katyal, 'Criminal Law in Cyberspace' (2001) Vol.149 University of Pennsylvania Law Review 1003-1011
[55] *Oxford v Moss*, [1979], Crime LR 119, Divisional Court
[56] N Meulen, supra, note 21
[57] United Kingdom Home Office, 2006 a

initiatives to prevent identity fraud and identity theft. In addition, in 2003, Home Office has established the Fraud Steering Committee and the Identity Fraud Forum to take measures to help combat identity theft.[58] Moreover, the UK legislature in the Fraud Act of 2006 implicitly considers obtaining another person's information by deception as a crime and the person may be guilty of identity theft.[59]

There are no special rules may be used to cover and prevent identity theft in the United Kingdom, however some rules may be found scattered among many laws, such as the Fraud Act of 2006, and the Computer Misuse Act of 1990.

1.1.4.9 Conclusion

To sum up, it is obvious that identity theft is a serious crime. It can be committed remotely via internet. It costs the states and individuals billions of dollars every year. In other words, crimes that are committed by using stolen identity cost individuals billions of dollars every year. In addition, individuals whose identities have been stolen suffer emotional damages and spend many hours to repair their credit history and their reputation. Moreover, it is difficult to discover identity theft because criminals use many and sophisticated methods to commit their crimes. Furthermore, they have the ability to conceal their crimes. Consequently, people rarely discover that they have been identity theft victims. Identity theft may be committed by one criminal or more than one either as principal participants or accessory participants.

Due to criminals use more sophisticated methods to commit identity theft and they have the ability to conceal their crimes, the law enforcement officials find it difficult to combat and prevent identity theft. In addition, the victims seldom discover that they were victims of identity theft and some victims do not report their victimisation to the police, thus the evidence may disappear.

It is important to state that all parties should cooperate with each other to prevent identity theft. Victims, financial institutions, report agencies and states should work together to prevent identity theft because laws alone cannot prevent it. Therefore, if

[58] N Meulen, supra, note 21
[59] Section 4(1) of Fraud Act of 2006 c. 35 (UK)

there is no cooperation between the parties of identity theft it may be continue to grow and threaten everyone without exception.

1.2 Identity Theft Historical Development

Identity theft is an ancient phenomenon, but it has come to us in a new fashion. The internet facilitates the commission of this type of crime and gives perpetrators new methods to commit it. These methods make it difficult to discover and detect identity theft, and then find sufficient methods to prevent it.

A person called Jacob, the first person who committed identity theft (as we know it), imitated his brother's identity in order to inherit the family estate. Jacob could get the family estate by using the impersonation way.[60] Impersonation as a way to commit identity theft means imitating a legitimate person with intent to defraud the individual in order to obtain personal benefits.[61] The impersonation method that was used by Jacob resembles the famous social engineering method that is now used by perpetrators to commit identity theft.

Another case of identity theft happened in the UK in 1450. Facts in this case were a person who worked as a doctor in England through the 1440s was accused of murder. In 1449, he fled to France. After one year, he came back to England under an assumed name,[62] and after a period of time changed his identity again to give more credibility to his status.[63]

Occasionally, the perpetrator steals another person's information to use it to obtain personal benefits or to escape from terrible life conditions or disposal for some obligations. For example, in 1771, a woman who worked as indentured servant was subjected to harsh treatment from her master. As a result of this harsh treatment, she decided to leave her former life and live in a new style of life full of luxury. To reach this type of life she used the British Queen's sister name and her address that she has

[60] M C Tenney, ed, *The Zondervan Pictorial Bible Dictionary*, (Grand Rapids, MI: Zondervan Publishing House1969); S K Hoffman and T G McGinley, Identity Theft (2010) 21 available at <http://legalchoice.net/freedocs/IDTR.pdf> viewed on 1 May 2011

[61] Hoffman and McGinley ibid 21

[62] ibid 22

[63] Helen M. Lyle, *Jack Cade's Rebellion 1450*, (George Philip & Son, Ltd., Historical Association 1950) 17

stolen when she had worked as a servant in the Queen's mansion.[64]

Even the deceased persons were not immune from identity theft. For instance, in 1917, Russian Czar Niclolas II was ousted in coup and some rumours were deployed throughout the world about his children's survival from death. After many years, numerous individuals tried to impersonate his children. Most impersonators tried to impersonate his youngest daughter Anastasia. A famous impersonation of Anastasia was in 1920 when a woman tried suicide, but was rescued by a patrolman, and then she was taken to a mental institution. In the mental institution, she told the doctor that her name was Anastasia; however, she could not prove her identity.[65]

In the twentieth century, the perpetrators have changed their methods to commit identity theft. They used sophisticated methods, such as creating false documents, forging, or stealing documents containing individuals' information to commit identity theft. For instance, a person who abandoned his study without getting a scientific certificate from any school held many important positions, such as a college lecturer, hospital orderly, and a schoolteacher, and he stole the medical credentials of a doctor and used his name; then he joined the Canadian Navy as a surgeon. In spite of having no formal medical practice, he performed many surgeries for soldiers in the Korean conflict. Eventually, He was discovered by the doctor's mother. After that, he was discharged from the Navy and deported from the country. Although the perpetrator had been arrested many times he continued to commit identity theft.[66]

With technological development, the perpetrators develop their methods to commit identity theft. For instance, in the beginning of the twentieth century, in the United States, the social security number (SSN) was adopted and used as a tool to achieve individuals' transactions. The purpose of the SSN was to help recover of the economic security that has been affected by the crisis at that time and ensure its stability in future. Consequently, in 1935 the United States' president enacted an Act to regulate the use of the SSN. The first Social Security card was issued in 1936; the use of which has been developed over the time. In addition, some companies had launched campaigns to their

[64] S K Hoffman and T G Mcginley, supra, note 60, 23

[65] S Lyzhina and Y Zaghid, (trs), 'The Unsolved riddle of princess Anastasia, Pravda (Russia)' (13 July 2004) available at <http://english.pravda.ru/history/13-07-2004/6156-nicholas-2/> viewed on 4 May 2011

[66] S K Hoffman and T G McGinley, supra, note 60, 25

manufacture. However, as mentioned above, perpetrators improved their technology to exploit the vulnerability associated with the SSN. Therefore, the risks of the misuse of the SSN increased over the years.

The SSN and the credit card that was issued provided another opportunity for the perpetrators to commit identity theft. After a few years, the credit card had become the main tool that might be used in individuals' transactions. In 1966 and before the holiday shopping season, the first identity thefts happened when many mails imitating mails of several banks had been sent to addresses in the Chilega area. Many individuals who received these mails had no credit cards. Moreover, many of them were children and pets.[67]

Nowadays, identity theft has become an epidemic and uncontrolled crime because individuals' information is available everywhere. In addition, the internet makes the commission of identity theft easier. Most individuals have information on the internet and they use the internet as a tool to achieve most of their transactions. The internet has become an indispensable tool in an individual's life. Consequently, most of their information may be found on it. Furthermore, with this technological development perpetrators can develop and use complex methods to commit identity theft. They may develop their ability to conceal their crime. As with any new technology the internet has strong and weak points, consequently the perpetrators may exploit these weakness points to steal people's means of identification. The first identity theft on the internet happened in 1971, when a Russian person attacked online the Citibank and transferred money from its customers' accounts to his personal account in Finland. He recruited many individuals to accomplish this operation.

In 1994, some members of a criminal ring used stolen usernames and passwords to log onto Citibank's computer network and rapidly conveyed millions of dollars to financial institutions situated around the world. Their crime was discovered when the bank officials noticed two doubtful wire transfers and reported the incident to the Federal Bureau of Investigation.[68] Most states have been plagued by the crime of identity theft. Criminals can use people's identities to commit other crimes, or achieve illegal

[67] S K Hoffman and T G McGinley, supra, note 60, 27
[68] S K Hoffman and T G McGinley ibid, 27

purposes for himself or for another person.

1.2.1 Identity Theft Is an Uncontrolled Crime

Nowadays, identity theft is a worldwide problem and it has grown fast. It costs states, particularly developed countries, billions of dollars every year. Crimes that are committed by using the stolen identity, for instance, cost American customers $50 billion annually.[69] In a survey that has been conducted by the Federal Trade Commission, it was stated that in 2008, approximately 9.9 million Americans fell victim to identity theft.[70] Crimes committed by using a stolen identity also cost the United Kingdom £2.7 billion. Identity theft targets more than 1.8 million victims.[71] The victims of crimes committed by the use of the stolen identity may be individuals, banks, financial institutions, and creditors.

Victims of identity theft suffer two types of effects or damages; financial damage that takes place when a perpetrator uses the victim's identifiers to open a new account in his name or perpetuate his existing account. Opening a new account in the victim's name is considered more dangerous than perpetuating his existing account because the victim in opening a new account occasionally does not know that she has become a victim of identity theft after a long time.

The victim of identity theft may spend much money to repair his credit card history and clean up his reputation that has been contaminated by identity theft.[72] Moreover, he may spend many hours to repair his credit history. Furthermore, the victim of identity theft suffers another type of damage, which is called emotional damage. The victim may suffer self-stress. If the victim falls victim to identity theft, he may lose his job and his credit history has polluted. Identity theft has side effects on a victim's family or society at large. There is no one immune from identity theft. It may affect all

---

[69] N Swartz, 'Will Red Flags Detour ID Theft?' (2009) Vol. 43 (1) Information Management Journal 38-41

[70] Kristin M. Finklea, 'Identity Theft: Trends and Issues' 2012, 1-28 available at <http://www.fas.org/sgp/crs/misc/R40599.pdf> accessed on 25 Jul. 2012

[71] National Fraud Authority, 'Identity Theft Costs UK £2.7 Billion Every Year' 2010 available at <http://www.attorneygeneral.gov.uk/nfa/whatarewesaying/newsrelease/pages/identity-fraud-costs-27billion.aspx> viewed on 2 May 2011

[72] K Zaidi, 'Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguards Personal Data in the United States and Canada' (2007) Vo. 19 (2) Loyal Consumer Law Review 99-150

individuals. There is no difference between an adult and a child, a healthy person, or a sick person, an ordinary person, or an important person, such as political, military members or even the president of the state.

The above facts show that identity theft is an uncontrolled crime in the world, particularly online identity theft because it can be committed remotely. It can be committed from or against a State like Iraq that has no specific law to govern it. There is no real information about the impact of identity theft in Iraq because people and most Iraqi scholars have no idea about what identity theft is and how it can be committed. Some Iraqi people may fall victim to identity theft, but they do not know.

When the author has interviewed some scholars, solicitors, and judges, he discovered that there is confusion between identity theft as a crime in itself and the use of stolen identity to commit other crimes. They stated that obtaining of another person's means of identification and then using it to commit other crimes is a crime of a false representation or it is a crime of what is called nowadays identity fraud.[73] However, even this case is not found in Iraqi legislation. All that has been conducted by the Iraqi legislature is that in the article 292 it considers the use of a false or real name to mislead judges as a crime, whereas in the article 456 of the Penal Code 1969, it considers the use of a false name as a false representation. In fact, the Iraqi legislature, judges, scholars, and people have no knowledge about the identity theft offence nor modern crimes that may be committed by using the internet.[74]

---

[73] Interview with Ahmed Farhan, a criminal judge in Cassation Court, Cassation Court, (Baghdad, 25 January 2013); Ali Al-Obeidi, a judge at Federal Court of Appeal of Baghdad Rusafa, (Baghdad, 27 January 20130, A Hardan, the Head of Diyala Criminal Court, Presidency of the Federal Court of Appeal of (Diyala, 5 February 2013); M Al-Zubaidi, a lawyer at Presidency of the Federal Court of Appeal of Baghdad/ Rusafa, (Baghdad, 27 January 2013); A Al Obeidi and A Al Ali, lawyers at Presidency of the Federal Court of Appeal of Baghdad/ Rusafa, (Baghdad, 27 January 2013)

[74] Saleh stated that Hanin Subhi who is a journalist has discovered in 2012 that she became a victim of identity theft. A hacker has stolen her personal information from her Facebook page, and then used it to extort her relatives to obtain money vouchers for his mobile. The journalist has complained against him at Court of Appeal Diyala. Unfortunately, Court of Appeal in Diyala has branded the incident as a fraud offence rather than identity theft, W Saleh, 'Hacking in Iraq: Extortion and Destroyed Government websites' Elaf Newspaper, February 24, 2012 available at <http://www.elaph.com/Web/Technology/2012/2/718471.htm> accessed on 2 June 2013; in her interview with some people, Saleh stated that the interviewees indicate many factors that may facilitate hacking and other cybercrimes in Iraq. For instance, they stated that due to absence of the control of government on the internet hacking now is considered a dangerous phenomenon. Recently, hackers have increased their attacks against government websites as well as people. Nowadays, Iraq is more susceptible to

Contrary to many countries that have enacted new laws to govern modern crimes, Iraq has no laws to deal with these modern crimes. There are no institutions like US and UK institutions to teach and advise people or warn them about being a victim of new technology crimes. Therefore, people in Iraq may fall victim to these crimes, particularly identity theft without knowing or having recourse to the laws that can be used to combat these crimes. On second of February 2013, for instance, a group of criminals called 'Kuwait hacker' attacked the website page of Iraqi prime minister and shut it down.[75] In addition, according to a report that has been conducted by Casber Spy Company, Iraq, among many countries, such as Saudi Arabia and Sudan, has been classified a high level of modern crimes risks.[76]

Another example, published in a newspaper called 'Muwatin', may explain how the Iraqi people can easily fall victim to technology crimes. In this example, a British woman contacted an Iraqi person and told him that she was a rich woman, who was ill and might die. Thus, she wanted to donate her money to Iraqi children because she knew that Iraqi children suffer from poverty. She asked the person to help her because

---

hacking than other countries because people and political members have no experience with the attacks by hackers. The hacking may be a result of competition between merchants. Every merchant endeavours to spy on his competitor to know confidential information relates to his transactions. The government should enact a new Act to organize the use of internet and the legislature should provide provisions in this Act that oblige internet providers to comply with this act and prevent the hacking attacks.

[75] R Behar, in Information Crimes, It is Necessary to Prepare Security and Judicial Measures for Searching, Investigation, and Trial, Justice News 5 February 2013 available at <http://thejusticenews.com/?p=9679> accessed on 23 Mar. 2013; a group of hackers called Saudi Arabian Army also have attacked in previous time the Iraqi republic precedency website. They severely attacked it and stressed that they will continue attack the website, Aswat Al- Iraq news June 25, 2012 available at <http://ar.aswataliraq.info/%28S%28exmpmvvvgvvbgn555gbtzu45%29%29/Default1.aspx?page=article_page&id=300354> accessed on 19 June 2013; Hackers also have attacked the website of former prime minster of Iraq. They have left a message that contains this sentence "we are not a tool that has been made in china we are a tool that has been made in Iraq. They warned him and requested him to do not play with them. That means he should not make political dispute with the government. If he still plays with them, he may play on his life. They have threatened him that they will destroy his website. It is important to mention that cybercriminals always attack members of government because they believe that they rich men. They may also believe that they are injustice in their treatment with people. Iraqna Ikhbariya Shabaka, June 25, 2012 available at <http://translate.google.com/#en/ar/Ikhbariya> accessed on 19 June 2013

[76] In this report, the company classified countries according to risks that they face into three groups: the first group is a high risk, in which internet users between 41% - 60% fall victim to internet crimes; the second group contains users between 21%-41% and finally the group, which contains internet users who less than 21%. N Al-Hakim, 'Electronic Crimes Cost Saudi Arabia Billion Rial' Okaz Newspaper, 27 January 2012 available at <http://www.okaz.com.sa/new/Issues/20120127/Con20120127473133.htm> viewed on 24 Mar. 2013

she did not know anybody there. She requested him to provide her with his account number to transfer the money to him, and then he would forward this money to Iraqi children. When she got his account number, she stole his money and emptied his account.[77]

[77] A Al-Darraji, 'With the Increasing of Invitation to Enact the Project of Information Crimes in Iraq' 6th of December 2012, Muwatin Newspaper, available at <http://www.almowatennews.com/news.php?action=view&id=43770> viewed on 24 March 2013; on May 20, 2013. The author has received the below email that contains the same story 'Hello dear, I want to use my money $7600000 for a charitable work in you country that will benefit the less privileged. I am very sick and my chances of surviving surgery operation is very slim, according to my doctor's information. And I do not want the bank to get hold of my money when I die, because I am a childless widow. If you can help me do this, please contact me immediately for more information about me and how to get to get the fund. I am impatiently waiting. Please, make sure you protect this message from the public. I do not want people to take advantage of this to start contacting me. I await the your reply at iva001@hotmail.co.uk Mrs. Ivanova.' also received this phishing email 'You have been declared the winner of the Five Hundred Thousand U.S.D ($500, 000, 00), which was won by your email address Australia, and here is your winning identification number: Winning no: GB8701/LPRC REF: 475061725
Lot: 7056490902 / 188
All participants were selected through a system of established voting form Nine hundred thousand e-mail mail from Canada, Australia, USA, Asia, Europe, Middle East, Africa and Oceania as part of our program international promotion takes place annually. Congratulations! Please contact Mr John Cliff Ferguson demand our agent for verification and procedure to obtain the prize. Email:johncliff_ferguson36@outlook.com
Send all this information after Mr John Cliff Ferguson immediately follow the procession.
THE QUOTE:
NAME: ... .
YOUR AGE: ... .
Marital status: ... .
PHONE: ... .
OCCUPATION: ... .
COUNTRY: ... .
Please kindly send your data to our claims agent Mr John Cliff Ferguson through the email address this(johncliff_ferguson36@outlook.com) is the person who will help you get your prize of $500,000,00
Best Regards
Dr Mrs. Alice Henry

1.2.2 The Importance of the Topic

As pointed out previously, there is a difference between identity theft and its effects or what is called crimes that are committed by using stolen identity. Identity theft is a crime committed when the accused obtains another person's means of identification, while its effects occur when the accused uses the stolen identity to commit other crimes. These effects or what are called crimes committed by 'using stolen identity' make identity theft as a serious crime because crimes committed through the stolen identity may affect individuals in their financial and their reputation as well as the economy of the state. Finance fraud is considered the notorious crime that is committed by using stolen identity. It occurs when the perpetrator uses the stolen identifiers to open a new account in the victim's name or perpetuate their existing account. The personal fraud also takes place when the perpetrator uses the stolen identifiers to get personal benefits from the government, such as health care or education.

In addition, the criminal may use the stolen identity theft to avoid a possible arrest by the police, criminal record, or escape a bad life situation and live in a new style of life. For example, he may give the victim's name or address to the police after he has committed crime to avoid arrest. On the other hand, he may use the victim's means of identification to escape his bad life and live in a new one.

The Iraqi legislature in articles 249, 287, 292 and 456 of the Penal Code of 1969 has emphasised the above effects and criminalised crimes that might be committed by using stolen identity, or false identity. In these legal texts, the Iraqi legislature has not stated the terms of identity theft or stolen identity. In effect, only the articles 292 and 456 of the Iraqi Penal Code stated what is called today 'the use of stolen identity, or false identity to commit other crimes.' Other articles deal with what is called fraud offences.[78] Identity theft taking place not only when the perpetrator obtains people's

---

Australian Lottery(Coordinator) 2013.'

[78] The Iraqi legislature in article 249 of the Iraqi Penal Code 1969 states "a person shall be punished by imprisonment for not more than three years or by a fine for not more than 300 Dinars or by both if he is questioned by a court or an investigative authority about his name and he gave it a name or character does not belong to him. The punishment will be imprisonment or/and a fine if he uses a known person; the legislature in article 287 states that a person is guilty of forgery if he another person's character to change the reality in a document; in article 292, the legislature states that "a person shall be punished by

names; it encompasses the obtaining of any means of identification, such as their address or date of births that may be used alone or in conjunction with other means by people to identify themselves.

It could be said that the reason behind the failure to use these two terms 'identity theft' and 'stolen identity' and the related failure to provide rules in the Iraqi Penal Code 1969 to govern identity theft is due to people own identities not always being used in their personal transactions. The Iraqi legislature has also not predicted this type of crime and the crimes that may be committed by using it. By the extrapolation of the above articles, it seems that the Iraqi legislature has attempted to enhance people's confidence in judicial decisions and protect their tangible property only. In addition, as it will be shown, identity theft is not committed against people's names or their characters only.

Consequently, for aforementioned reasons, this study will provide a real picture on how this crime is committed, what can be used to commit it, and how other jurisdictions curb identity theft. It will be more important for the Iraqi legislature, judges, scholars, and even general population. The study will also be a revelation and vehicle for the Iraqi legislature to evaluate and develop its theft offence laws to protect people's means of identification and their financial information from being unlawfully obtained and then used it to commit other crimes or enact a new law to deal with identity theft. The study will also assist the Iraqi legislature to evaluate and reformulate the project of Information Crimes 2011 in order to govern crimes that are committed by using technology.

The information collected by this research will benefit not only the Iraqi legislature; but police, prosecution office, judges, and academics as well. It may assist them to update their knowledge about the new crime and its challenges to social immunity. The knowledge that may be obtained of this study will also provide a mechanism of protecting people's means of identification, the economy, and society at large.

Recognising the problems, which are caused by identity theft, outlined in this study will

---

imprisonment or by a fine for not more than 300 Dinars or by both if he uses a false name or character to get a formal licence or ticket card; in article 456 of the Penal Code 969, the Iraqi legislature states that a person shall be punished by imprisonment if he has enabled to receive or transfer another person's property by using: 1. A false name or character.

provide a better understanding of those problems and will create opportunities for problem-solving in a broader perspective in which the solution of identity theft may provide guidance to resolve other problems. For instance, it may provide solutions for methods that are used to commit identity theft, identity fraud, and computer crimes. The importance of the topic can also be seen where no legal research has been conducted about this crime, as a PhD thesis.

1.3 A Perspective of Identity Theft in World Jurisdictions

In some states, such as the United States, the main victim of identity theft is financial institutions, banks and creditors rather than individuals because these institutions incur monetary effects while individuals do not incur monetary effects. Some States were more susceptible to the risks of identity theft than other states. As a result, some states, such as United States, Canada, and Australia, have enacted special laws to prevent identity theft, whereas other states, such as France consider the use of another person's information without his consent as a type of fraud. Although in other states, such as the United Kingdom, identity theft is widely committed yet it has not enacted specific Acts to combat identity theft.

Recently, identity theft has invaded some Arab countries, such as Egypt, Syria, Bahrain, Sudan, Saudi Arabia, Arab United Emirates, and maybe Iraq.[79] If identity theft invades

[79] Egypt, Syria, and Bahrain have no specific law to deal with identity theft, whereas United Arab Emirates, Sudan, and Saudi Arabia have enacted new laws to deal with identity theft. These laws do not directly deal with identity theft, but each one of them contains an article that deal with identity theft. The Combating Information Technological Crimes Law of United Arab Emirates 2006 (2) for instance, in article (12), states that everyone who uses the internet or any means of information technological without right to get credit cards numbers or its data or any electronic credit shall be punished by imprisonment and fine. If he intends to get these numbers to use them to obtain another person's properties or any services that may be obtained by these properties shall be punished by imprisonment for not less than sixth month or by one of them. The punishment will be imprisonment for not less than one year and a fine for not less than 30000 Dirham or one of them if he uses these numbers to obtain for himself of another person the properties of somebody else. The previous law has been amended by the Information Technological Crimes Law of United Arab Emirates No. 5 of 2012; the article (12) of the Sudan Information Crimes Law of 2007 states that everyone who uses the internet, one of computer devices or any device likes it to access the credit cards numbers or their data or any card likes it with intent to get another person's information, his properties or any services that these numbers or data to facilitate them, shall be punished by imprisonment for not more than five years and fine or by one of them. The Saudi Arabia Electronic Information Crimes Law No. 79 of 2007 (4) states that shall be punished by imprisonment for not more than three years or by a fine for not more than two millions Rial or by one of these punishment everyone who commits one of below crimes: 2. Access without probably legally

Iraq, it is considered a new crime in Iraq. Contrary to the above developed countries, Iraq has no specific law to deal with identity theft. Consequently, there is no clear definition for this crime in the Iraqi and other Arab countries legislation. Theft offence laws that are in place have been enacted before the act of the unlawful obtaining of a person's means of identification and then using it to commit crimes has become an issue. The current Iraqi theft offence laws have remained static to protect tangible property while intangible things (individuals' information has become more susceptible to theft) are not covered. Theft of a person's information was beyond what the Iraqi legislature of theft offence laws could have envisaged at the time of enacting these laws.

Recently, the Iraqi Government has proposed a project called the Information Crimes Project of 2011. This Project does not contain provisions that deal with identity theft as a crime. Consequently, this project cannot protect people's means of identification from the act of the illegal obtaining and then using to commit other crimes. This project has failed to protect people not just from identity theft; it has failed to protect them even from other computer crimes. Thus, these laws lack provisions that deal with theft of individuals' information. This situation may put Iraq at risk of being identity theft's safe haven. This may also put the rest of the world at risk by creating a jurisdiction safe haven for criminals. Criminals who commit identity theft may easily evade the liability of this crime due to the gap in both Iraqi theft offence laws and the new project of Information Crimes 2011.

Due to this lack of legal provisions, courts in Iraq and other Arab countries may misunderstand the nature of the illegal obtaining of another person's means of identification, and then using it to commit other crimes. Misjudgements may be found among judgements of these courts. They do not know how to deal with identity theft as a separate crime. They sometimes rule the accused on the crime that is committed by using a stolen identity. In a recent case that happened in Arab United Emirates in 2003, for example, the accused who was a worker in a Holyuod restaurant used a skimmer device to copy the credit card information of the client and then gave the device to

---

permission to a bank and credit data, or data related to possessed documents to get data, information, properties or anything that these document may facilitate it. Although, these laws do not deal with people's means of identification they are considered good steps that are taken by these jurisdictions.

another person who also gave it to a third person. The third person transferred the information from the device to another person who used it in fraudulent activities. He could steal 10,868 Dirhams from the victim's account. Dubai courts treated the co-complicities as having committed fraud offences rather than identity theft.[80]

The question that may rise here is how this crime can be countered by Iraqi judges given the lacuna in Iraqi laws to combat identity theft. Is a new needed law to govern it? If the answer is 'yes' how can the Iraqi legislature formulate this law? Does it need to borrow provisions from other jurisdictions because they have no experience about crimes that are committed against intangible properties, particularly crimes committed by using the internet and how can it be countered?

1.4 Thesis Statement

Information or confidential information is intangible material. People's means of identification is a type of this information, which has recently become very susceptible to illegal activities. People's means of identification can be obtained through illegal activities without consent, and then used to commit or facilitate other crimes. One of these illegal activities is theft. Therefore, a new crime called identity theft has appeared. Identity theft is called a millennium crime. It grows fast growth and can potentially cost states billions of dollars. It is committed against a specific type of intangible material. With absence of a specific law in Iraq to govern this crime and due to the nature of the means of identification, difficulties arise as to whether traditional theft offence laws in Iraq can be applied to the act of the unlawful obtaining of a means of identification.

Generally, theft offence laws in Iraq have been enacted to deal with tangible property. To be subject to theft, tangible property should be taken by physical action with intent to permanently deprive the owner of his property. As a result, a debate has been arisen as to whether the act of the illegal obtaining of another person's information will fall within the scope of theft offence laws. This debate focuses on difficulties that may be faced when the current Iraqi theft offence laws are applied to identity theft. These difficulties consist of whether personal information can be subject to physical theft. The second difficulty is whether an individual's means of identification can be considered as

[80] *K* and *Others v. Criminal Court First Degree*, Dubai Courts, Fifth Criminal Authority (2004) [2004]

property. Finally, another issue arises whether identity's use means that the owner would be deprived as a consequence of this use.

When the above difficulties have been analysed it will clear that the current theft offence laws in Iraq may be inadequate to govern identity theft. As a result of the inadequacy that may be found in theft offence laws, the interpretation of legislation and the role of a criminal judge to extend existing Iraqi theft offence laws (or create a new law) needs analysing. However, attempting to extend existing theft offence laws (or creating new offences by the judge) could be contrary to the principle of legality that is found in most civil law systems. Overall, it will be seen that the legislative interference seems to be necessary to fill the potential gaps that may be found in existing legislation.

As part of the research, this thesis will examine whether existing Iraqi theft offence laws (with reference to the USA and UK legislation) are adequate to deal with identity theft or not. For this purpose, theft offences in Iraqi law will be analysed. Theft offence laws in Iraq raise many difficulties that may be faced when they are applied to identity theft offence because these laws have been enacted to deal with movable tangible property only, whereas personal identifiers are intangible. To scrutinise the Iraqi theft offence laws, the relevant UK and US legislations will be also discussed to examine how they deal with this new type of crime.

In addition to this, the role of the Iraqi criminal judge to interpret the statute of theft offence laws to extend the scope of them to govern identity theft shall be discussed. Since the principle of legality may be an obstacle that prevents the application of the theft offence to identity theft offence, the author will explain how Iraqi criminal judges interpret the current theft offence laws. He will also examine whether the criminal judge can interpret theft offence laws in a manner that adequately extends the current theft offence laws or creates new laws to govern identity theft. Alternatively, that may constitute breaching of the principle of legality.

1.5 Scope of the Study and Limitation

This study has focussed on the Iraqi jurisdiction and its need for legal reform. The UK and US jurisdictions were selected as a reference because the US is already well advanced in their experience in responding to identity theft. While in the UK, although

there is no specific law that deals with identity theft as a separate crime, judges have significant experience in dealing with crimes committed by using identity theft. In addition, the two developed countries are chosen for this study due to a number of additional reasons:

1. The UK and the US are developed countries and the crime of identity theft has appeared here. They combat this crime by either enacting legislation or through a judicial solution.
2. As mentioned previously this crime has only recently caused problems in Iraq, therefore the Iraqi judges and scholars have no experience about how they can find solutions to combat this type of crime.
3. The legal system in both the US and the UK depends on common law, thus judges in these countries have more experience in dealing with the inadequacy that may appear in their legislation, so they can sometimes interpret the law extensively to ascertain the spirit of it and protect people.
4. The US legislation has suffered from inadequacy, but the US legislator enacted two laws to deal with identity theft and protect people's means of identification. Accordingly, Iraq may benefit from the merits of these two US laws to combat identity theft and evaluate its legislation.
5. Courts and judges in UK and USA have more experience dealing with identity theft because it has appeared in these countries' laws for more than two decades. As a result, it is considered a resource that may help the Iraqi criminal judges to know how they can overcome any inadequacy that may be found in the Iraqi legislation, particularly theft offence laws with respect to identity theft.
6. The UK is the country of the author's study; consequently, it is important to apply the legal experience of this country to Iraq.

The USA also experienced a situation in which Iraq now finds itself. There was no US specific law addressing identity theft as a crime before 1998. In 1998, the US legislature enacted laws to address identity theft, thus, these frameworks may provide benchmarks for Iraq. Despite this, the UK is still in the same situation as Iraq in that it has no specific law addressing identity theft, but has many laws indirectly dealing with identity theft. These laws may have merits and demerits, however, the Iraqi legislature may

benefit from them. As a result of the absence of a specific law to govern identity theft, the current Iraqi theft offences laws will be examined to assess whether Iraqi judges can apply them to identity theft.

The specific nature of the individuals' information and the methods that are used to obtain this information trigger difficulties that may be faced when existing Iraqi theft offence laws are applied to identity theft. Three difficulties can be imagined when existing theft offence laws are applied to identity theft: is a person's means of identification property, can this means of identification be subject to physical taken and finally is the person whose identity has been stolen deprived of it. By analysing the current Iraqi theft offence laws the author will invoke the old experience of both UK and US to explore how judges in these two jurisdictions deal with the application of traditional laws to new crimes not governed by these laws.

Two consequences may arise from the analysis of the current theft offence laws: either these difficulties are not found and Iraqi judges can apply the current theft offence laws to govern identity theft, or they are found and the current theft offence laws are inadequate to govern identity theft. The latter consequence gives rise to an issue whether the Iraqi criminal judges can extend the current theft offence laws in a manner in which these laws can be applied to the person who wrongfully obtains another person's information without his consent, and then uses it to commit other crimes, (or whether Iraq needs to create a new Act).

However, the above question may raise an inquiry as to whether the principle of legality that is stipulated in Iraqi legislation stands as an obstacle to prevent criminal judges from extending existing theft offence laws (or from creating new laws) to govern identity theft. To examine the above issues and answer the questions one should analyse the current theft offence laws and the interpretation of statutes by judges to scrutinise whether judges can apply the current theft offence laws to identity theft or they need to interpret these laws to extend the scope of them to govern it. Finally, from the analysis of the methods that can be used by the judges to interpret the current theft offence laws it will be apparent whether the principle of legality prevents the criminal judge from extending the current theft offence laws (or from creating a new Act) to govern the illegal obtaining of a person's identity not governed by these laws. Thus, the Iraqi

legislature might need to enact new laws to govern identity theft and fill in the potential gap in the legislation.[81]

1.6 Summary of the Problem

As mentioned previously, identity theft is a fastest growing crime in some States. It has great effects on all parties whether individuals, governments, companies and financial institutions. In addition, it is committed through two types of methods, sophisticated methods (such as phishing, spam, or Trojan Horse) and unsophisticated methods (such as dumpster diving, mail stealing or stealing from inside workplaces). Some of these methods stand alone as crimes and they need a specific Act to criminalise them. Identity theft is committed against personal information, which has a specific nature. This specific nature of personal information may give rise to an issue whether the conventional provisions of theft are adequate to prevent identity theft. In addition, it may give rise to an issue whether the criminal judge, by interpreting the current theft offence laws, can extend the law (or create a new law) to govern identity theft.

If the country wherein this crime takes place, such as Iraq, adopts the principle of legality that prevents a judge from extending the existing law (or from creating a new one) to govern it, the requirement to the legislator to enact a new Act that criminalises this crime to protect people becomes an urgent issue. Due to sophisticated methods used to commit the identity theft it is considered a crime across national boundaries. Many jurisdictions may be involved with this crime; therefore, it may raise the extradition issue. However, jurisdiction and extradition issues are beyond the scope of this this.

1.7 Hypothesis and Objectives of the Study

The thesis has the following hypothesis: the current theft offence laws and the Information Crimes Project of 2011 are inadequate to govern identity theft. The main objective of this study is to scrutinise whether the current Iraqi theft offence laws are adequate to govern identity theft. Before examining this objective, the study attempts to examine whether identity theft has unique characteristics, which may present great challenges when existing Iraqi theft offence laws are applied to it.

[81] This study does not deal with crimes that are committed by using stolen identities, procedures that are needed to prove identity theft crimes against the criminal or procedures that are used by some companies, such as verification to distinguish between real and imitator person.

To explore whether identity theft has unique characteristics the definition of identity theft, types of identity theft, and the differences between identity theft and other crimes will be discussed. In addition, the study attempts to give an idea about the elements of identity theft or methods that may be used by perpetrators to commit identity theft. The study tries to shed light on the participation in identity theft that takes place widely, but receives relatively little attention from scholars. As pointed out previously, identity theft that relates to the internet consists of so many activities that one perpetrator cannot accomplish them alone, thus, he or she should look for co-perpetrators to help him or her to achieve this task, yet the legislators have left the regulating of participation in identity theft to the existing rules.

Examining the elements of identity theft is considered important to help understand whether identity theft falls within the scope of the current theft offence laws. Accordingly, the second objective of this study is to analyse and evaluate the role of the criminal judge in interpreting existing Iraqi theft offence laws to examine whether the judge can fill in the gap or gaps that may be found in these laws. The third objective is to examine and evaluate the extent to which the Iraqi legislature can adopt or borrow provisions from either US or UK legislation (or from both) in order to enact a new comprehensive law to criminalise identity theft. The final objective is to propose amendments to existing laws and enact new laws.

1.8 Methodology

Since this study focuses on Iraqi legislation and its inadequacy to combat identity theft with US and UK legislation as a reference, it is, however, not a comparative study in traditional term. The US and UK jurisdictions have been chosen for reasons that are stated previously, to explore how they deal with identity theft. In the past, neither the US nor the UK had laws dealing with the specific act of identity theft as a crime. However, the US has recently enacted two laws to deal with act of identity theft, while the UK, like Iraq, still having no specific law that deals with identity theft. In the UK, judges look at various laws to find rules to combat identity theft. The focus of the study is on Iraqi legislation to determine whether Iraqi laws are adequate to govern identity theft. Critical analysis will be undertaken of the current Iraqi theft offence laws, with US and UK legislation as a reference, law cases and academics' literature related to this

topic that are taken from law books, journal articles and various reports.

1.9 Thesis Plan

This thesis aims to scrutinise whether the Iraqi theft offence laws and the Information Crimes Project of 2011 are adequate to govern identity theft. Two types of legislation have been chosen as a reference: US and UK legislation in order to propose improvements in the current Iraqi theft offence laws and the project of 2011 to enable them to respond effectively to challenges that brought about by identity theft. To answer the above question the thesis has been structured into seven chapters.

Chapter One includes the introduction, importance of the topic, thesis statement, background of identity theft including the history of the crime, the objectives of the study, the methodology, and plan of the thesis.

Chapter Two covers some preliminary considerations crucial to understanding the problem. It focusses in this chapter on the concept of identity theft, determines the distinctive features of this legal phenomenon, and provides the definition of identity theft. There is no universal definition of identity theft. As a result, the author assesses definitions found in the relevant academic literature as well as US and UK legislation chosen as a reference. In this chapter, the study also tries to distinguish between identity theft and other crimes, such as identity fraud and identity crime. Characteristics of identity theft will also be discussed. Identity theft targets everyone in society. It does not differentiate between individuals. Consequently, victims of identity theft and its effects on them have also been discussed in this chapter.

Chapter Three examines and analyses the elements of identity theft as they have been broken down by academic literature and other jurisdictions' laws. Identity theft as any crime consists of two well-known concept elements: *actus reus*, and *mens rea*. The *actus reus* refers to an illegal act that is represented by methods that are used to commit identity theft and the use of or transferring of a person's means of identification.

The *mens rea* consists of knowingly using means of another person's identification and without consent. However, there is a third element, which is culled the subject matter of the crime. It consists of two elements the means of identification and belonging to

another person. These elements have unique features that make identity theft as a specific crime that calls for a specific law to address it. From the analysis of the elements of theft, the author observes that there is no indication that refers to these elements as they are stated in scholarly literature. The US legislature adds the term "without unlawful authority" as an element to the *mens rea* of identity theft. In effect, as it will be shown in Chapter six that the US legislature criminalises the aftermath stage of identity theft commission, thus the term "without unlawful authority" is not an element of identity theft.

In this Chapter, this study attempts to illustrate these elements. The illustrating of the methods that are used by criminals to commit identity theft takes a large amount of this chapter. Traditional or non-sophisticated and non-traditional, or sophisticated methods can be used to commit identity theft. Some of these methods may need to be criminalised by a specific law because they stand alone as crimes.

In Chapter Four, challenges that may be faced when the current Iraqi theft offence laws are applied to identity theft will be discussed. The study shows that three challenges may be faced when these laws are applied: the physical taking of another person's means of identification; the labelling of this means of identification as property; and the intention to permanently deprive the person of his means of identification. There is debate between scholars as well as judges with respect to each one of these challenges. This debate will be discussed in detail in this chapter. A main point that is stated in this debate is existing Iraqi theft offence laws are inadequate to govern identity theft and the issue should be resolved either by a decision from the court or the legislature should enact a new Act to govern this crime. Accordingly, these two suggestions will be subjects in chapters five and six.

The judicial solution to overcome the legislative inadequacy that is proved in chapter four will be discussed in chapter five. The judge can resolve the legislative inadequacy by either extending the current theft offence law (or by creating a new one) to govern identity theft. The criminal judge can extend the current theft offence laws (or create a new one) by interpreting the current theft offence laws or by using analogy. However, in some jurisdictions, such as Iraqi legislation, extending the current law (or creating a new one) may be obstructed by the principle of legality. Therefore, the interpretation of

legislation and the principle of legality will be illustrated in this chapter.

Chapter Six includes an analysis of the legislative solution that is provided by the UK and the US legislation to scrutinise whether the Iraqi legislature can adopt or borrow provisions from either the UK or the US legislation (or from both) to enact a new law that governs identity theft. The UK legislation has no specific law to deal with identity theft because the UK legislature does not consider identity theft as a separate crime. However, British courts can use existing laws, such as the Data Protection Act 1998, Theft Act 1968, Fraud Act 2006 and the Computer Misuse Act 1990, to deal with identity theft. The US legislature enacted two laws to deal with identity theft: the Identity Theft and Assumption Deterrence Act 1998, and the Identity Theft Penalty Enhancement Act 2004. Therefore, these laws will also be discussed in this chapter.

Finally, Chapter Seven contains conclusions to what has been addressed in the thesis. In addition, in this chapter, some recommendations will be given, which may be appropriate to assist the Iraqi legislature when it seeks to enact a new law to govern identity theft.

Chapter Two:

The Main Features of Identity Theft – Its Distinction of Other Crimes, Perpetrators and Victims

Introduction

In Iraq, there are three main types of laws deal with crimes, which may be committed against people's properties: Theft Offence Laws, Fraud, and Betrayal Trust Offence Laws. Some scholars, judges, and legislatures in other jurisdictions brand taking another person's means of identification as theft. As stated previously, Iraqi having no specific law deals with the act of the illegal taking of another person's means of identification. Consequently, Iraqi legislation lacks the accurate legal definition of this crime. From a legal point of view, to criminalise an illegal act it should be defined precisely. Additionally, according to the principle of legality the elements of an illegal act should be accurately determined.

However, before exploring whether the criminalisation of identity theft needs a specific law it is necessary to examine whether Iraqi judges and scholars can look into one of the above laws, which may be appropriate laws that can be used to govern the theft of another person's means of identification. Theft offence laws seem to be most applicable to Iraqi judges and scholars to find out provisions from them that govern identity theft because these laws are the only laws that deal with the taking of another person's property without his consent.[1] By doing so, it is necessary to examine whether the definition that is stated in the current theft offence laws is adequate to encompass the illegal obtaining of another person's means of identification.

In addition, Iraqi government has presented the Information Crimes Project of 2011 that deals with crimes that are committed by using the internet. With respect to explore definition of identity theft in Iraqi laws, it is necessary to search into the provisions of

[1] Fraud Offence Laws deal with the taking of another person's property with his consent by using fraudulent activities, such as using false name or using false representation. See article 456 of the Penal Code No. 111 of 1969; Betrayal Trust Offence laws deal with the taking of another person's property that is submitted to the accused according the one of trust contracts. In betrayal trust offences victims consensually and voluntary handles his property to the accused according to these contracts, while in identity theft the accused always takes another person's means of identification without that person's consent, article 453 of the Penal Code No. 111 of 1969

the new project to scrutinise whether these provisions contain a definition for identity theft as a crime.

The consequence that may be resulted from of the above analysis will be either positive or negative. If the answer is positive that means identity theft is defined in the current theft offence laws or in Information Crimes Project of 2011, however, if the answer is negative that means identity theft is not defined and needs to be defined. To overcome the negative consequence of the analysis and determine an accurate legal framework of identity theft, the definition of identity theft in scholars' literature and other jurisdictions will be discussed in this chapter too.

As a result, this chapter intends to examine and discuss identity theft drawing from different legal frameworks. It begins by exploring the situation in both existing Iraq theft offence laws and Information Crimes Project of 2011, and then extends to explore various definitions of IT, and how countries like the USA, Canada, UK, and Australia can conceptualise identity theft. The USA and the UK have been chosen as a reference, while Canada and Australia have been chosen because the legislatures in these two jurisdictions define identity theft in a way that is slightly different from the USA and that may assist the author to espouse an accurate definition of identity theft. This chapter also contains recapitulating about features of IT and distinguishing it from other crimes. Subsequent sections examine IT victims and perpetrators relationship. Therefore, the chapter will be divided into seven sections.

2.1 Definition of Identity Theft:

The definition of identity theft will be examined in Iraqi legislation, the Academic Journals and other jurisdictions.

2.1.1 Exploring the Definition of Identity Theft in Iraqi Legislation:

As stated previously, there is no definition to identity theft in Iraq because it has no specific law to deal with identity theft. As a result, the study attempts to examine whether the definition of traditional theft that is stated in existing Iraq theft laws encompasses the illegal obtaining of another person's means of identification.

There is no obvious situation in Iraqi legislation about the obtaining or the use of

another person's means of identification without their consent to accomplish illegal purposes. In Iraqi legislation, theft is defined as intentionally misappropriation of a movable property that is owned by a person non-perpetrator.[2] The Iraqi legislature states some examples of an intangible property that may be a subject of theft. It stated for example, that electric power is a subject of theft if it is appropriated by another person. The Iraqi legislature also considers trees as a stolen subject merely it is separated from ground. However, this definition does not refer to the obtaining of another person's means of identification as subject to theft because the Iraqi legislature does not state this information in the definition of the theft offence.

In 2003, after the US's invasion of Iraq, Iraq has become a sense of many crimes, such as terrorist operations, where the current Penal Code 1969 is inadequate to combat them and criminal judges could not find solutions to these crimes. As a result, the Iraqi legislature enacted the Terrorism Act No. 13 of 2005, and then it has proposed the Information Crimes Project of 2011.[3] This project has been abolished by Iraqi

[2] Section 439 of the Iraqi Penal Code No. 111 of 1969

[3] This Project has been criticised by many scholars and judges. It is argued that this project should be amended according to international standards. It should also take into account the specific nature of information crimes. The Iraqi legislature cannot amend this project because they have no background to deal with the internet. Judges cannot also combat these types of crimes because they have not a good experience in crimes that are committed by using the internet or by using to commit other crimes. R Bhari, 'In Crimes of Information It Is Necessary to Provide Security and Judicial Measures in Search, Investigation and Trial, the Modern Crimes Constitute Challenge to the Iraqi Security 2013', 5/2/2013, available at <http://thejusticenews.com/?p=9679> accessed on 15 March 2013. In addition, in 27/12/2012, the UNESCO Iraq Branch held in Baghdad a conference to evaluate the Information Crimes Project. In this conference, many scholars and judges have been invited to attend this conference. In this conference, Al- Musawi is a judge and a lecturer in Iraqi judicial institution argued that this project is violation of constitution and when somebody reads its articles, it seems to him that the contents of this project have been written by non-specialists, such as security and military officers. It is a means to control the internet only, K Al-Isawi, 'UNESCO Iraq Branch Held a Conference to Discuss Information Crime Project', Al-Marsad News, available at <http://www.almarsadnews.org/security-and-policity/6319.html> accessed on 21 Jun 2013. In this conference, the head of the parliamentary Culture and Media Committee in Iraqi Parliament also stated that the Project of 2011 is an unsuitable project and I have asked the parliament to abolish it; it is said that there is unconformity between this project and the constitution. It mentions articles deal with definition, but it does not state the rights. It mentions some illegal activities, such as crimes against the safety of the state that are governed by the current Penal Code 111 of 1969 and this may lead to confuse the judge. There is overlap between its provisions and the Terrorism Act 2005. Moreover, it extends the punishment to govern persons rather than the accused. It makes the Federal Court of Appeal Baghdad/ Rusafa only as a court to deal with crimes that are governed by it and that may be difficult to judges, the accused, and even the witnesses who live far from Baghdad. Z Abood, 'an Opinion in Draft of Information Crimes Project of 2011' Judicial Magazine 3/12/2012 available at <http://www.iraqja.iq/view.1705/> access on 13 March 2013

parliament because many civil organisations either inside or outside the Iraq have rejected it. With respect to crimes that are committed against personal information, this project if has been enacted it will curb some cybercrimes, but not the unlawfully obtaining of another person's means of identification. It seems from the extrapolation of the 31 articles, which are provided in this project that the Iraqi legislature in this project criminalises some unlawful activities. For instance, it criminalises creating false website to carry out terrorist operations,[4] forging smart credit cards or other documents,[5] protecting the integrity of computers,[6] criminalising gambling and pornography,[7] using false or names that are not belong to the person to defraud and misleading people.[8] The infringing of intellectual property has also been criminalised in this subject.[9]

However, it appears that this project does not contain provisions, which can be used to govern the unlawfully obtaining or using a person's means of identification without their consent with intent to commit other crimes. Consequently, it does not define the unlawful obtaining of another person's means of identification. As a result, it is necessary in the next section to examine the definitions of identity theft in both academic commentaries and some jurisdictions to provide a real picture of definitions stated in them about identity theft and appreciate whether one of these definitions can be espoused by the Iraqi legislature when it intends to enact a new Act to govern identity theft.

2.1.2 Examine the Definition of Identity Theft in Academics' literature and Jurisdictions:

In this section, identity theft will be defined and determined from two aspects: (1) academic commentaries and (2) legislation. Definitions in both academics' literature and legislation that relate to this crime will be examined in order to assess whether the Iraqi legislature can adopt one of them or not, otherwise, to propose an adequate definition of identity theft that can be adopted by Iraqi legislation.

[4] Section 4 (1) of the Iraqi Information Crimes Project 2011
[5] Section 8 (1)(b) ibid
[6] Section 14 (1, 2, 3) ibid
[7] Section 22 (1, 2) ibid
[8] Section 18(2) ibid
[9] Section 21(1, 2) ibid

2.1.2.1 Definition of Identity Theft in the Academic Journals:

There are various different definitions of identity theft. IT is a term referring to the unlawful use of another person's means of identification by a perpetrator to commit other crimes. IT consists of two terms; (1) identity, which can be defined as some features that individuals use to distinguish themselves and use, take unique pride in or view as a social consequential.[10] It is the answer to the question, who are you or who am I, and (2) theft, which is a term that refers in general to an act that refers to carry away, misuse, or take away other persons' properties whether tangible, or intangible without their consent. Having given an idea about the two elements of the term of identity theft, now let us know what is identity theft?

Identity theft is 'any impersonation of a specific individual'.[11] However, the definition cited above does not provide sufficient elements or determinants of identity theft because identity theft may occur by several methods and affect more than just individuals. In addition, identity theft takes place when a person obtains another person's means of identification and not when he uses this means to impersonate that person.

Identity theft is also defined as a term that is used to describe a variety of illegal acts involving theft or misuse of personal information,[12] such as a social security number, mother's maiden name, or password to perpetuate an existing account or to open a new account. In addition, it is defined as the misuse of another individual's means of identification information to commit fraud.[13] This definition has limited identity theft with an unlawful act that causes fraud only while there are other types of unlawful activities that the stolen persons' identities can be used to carry them out, such as using

[10] J D Fearon, 'What Identity (as We Now Use the Word)?' 1999, 2 available at <http://www.stanford.edu/~jfearon/papers/iden1v2.pdf > accessed on 25 May 2011

[11] L LoPucki, 'Human Identification Theory and Identity Theft Problem' (2001-2002) Vol. 80 Texas Law Review 89-134

[12] K Baum, 'Identity Theft' (2004) Bureau of Justice Statistics Bulletin 2006 U.S. Department of Justice Office of Justice Programs, 2 available at <http://www.bjs.gov/content/pub/pdf/it04.pdf > accessed on 20 June 2013

[13] The President of Identity Theft Task Force, 'Combating Identity Theft: A Strategy Plan' 2007 section 2 available at <http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/IdentityTheft/DownloadableDocuments/Combating_Identity_Theft_A_Strategic_Plan.pdf> accessed on 29 May 2011

another person's identity to avoid criminal record or to dispose of a bad life situation.

Moreover, Lynch[14] defines the term of identity theft as a term that describes the use of another person's means of identification for fraudulent purposes. This definition is inacceptable because it refers to the use of the means of identification after it has been stolen to commit fraud; while there are many other illegal activities that this means of identification can be used for achieve them. In addition, identity theft occurs before the use of another person's means of identification to commit other crimes. The use of means of identification is an effect of identity theft. It may be a preparatory act to commit other crimes, but not identity theft itself.

Identity theft has also been defined as the locating and using of someone else's clean identity by a thief to commit other crimes.[15] It might be argued that this definition does not refer to aiding or abetting other persons to commit a crime. Cavoukian[16] defines the identity theft offence as obtaining key pieces of another person's information in order to impersonate him and carry out different crimes in his name. This information may include a passport number, mother's maiden name, PIN, and a driver's license number.

It could be said that it is hard to explore a comprehensive definition for identity theft because the term is broad and each researcher looks at it from his/her own perspective. For instance, the National Crime victimization Survey that issued in 2006 by Federal Trade Commission of America, revealed three definitions of identity theft. The three definitions were in accordance with the subject that the identity thief targets,[17] such as the use of or attempt to use an existing credit card, using, or attempt to use an existing account, such as cheque, or misuse other persons' personal information to get a new

[14] J Lynch, 'Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks' (2005) Vol. 20 Berkeley Tech. J.L 259- 260

[15] L Cradduck and A McCullagh, 'Identifying the Identity Thief: Is It Time for a (Smart) Australia Card' (2007) Vol. 16 (2) International Journal of Law and Information Technology Oxford University Press 125-158

[16] A Cavoukian, 'Identity Theft: Who's Using Your Name?' (1997) Information and Privacy Commissioner/ Ontario, 2 available at <http://www.ipc.on.ca/images/resources/idtheft-e.pdf> accessed on 2 June 2011

[17] K Baum, supra, note 12; H Copes and L Veraitis, 'Identity Theft' (2009) 564-571 (565) available at <http://www.uk.sagepub.com/haganintrocrim7e/study/features/articles/HB14.1.pdf> accessed on 23 Jun. 2011

account, mortgage or to carry out a crime.[18]

Moreover, words that are used by the scholars are unable one to depict the true concept of identity theft. For example, the National Crime Victim Survey does not resolve the problem that may take place when the perpetrator appropriates a credit card to buy goods, and then abandon it. In addition, some researchers limit the definition to a fraction of the subject, such as the criminals of identity.[19] Others employ their definitions of identity theft for some of the identity theft activities and leave the others or treat them as a separate crime.[20]

Giving the concept of identity theft in academics' perspectives above, let us examine how the act is being perceived or defined in different countries.

2.1.2.2 The Definition of Identity Theft in Legislation:

There is no agreement about identity theft as a crime among the countries of the world. Some countries, such as France consider it as a form of fraud[21] and a person who uses another person's information without their consent for illegal purposes s/he may be liable for civil compensation. However, other countries, such as United States, Canada and Australia consider it as a crime. United Kingdom does not consider identity theft as a separate crime. On the other hand, some countries, such as Iraq and other Arab countries do not have provisions to govern identity theft. Therefore, there is no clear definition of identity theft. Below definitions of identity theft in the legislation of some countries (US, UK, Canada, and Australia) will be reviewed.

[18] M Tonry, *The Oxford Hand Book of Crime and Public Policy* (New York Oxford University Press 2009) 249

[19] H Copes and L Veraitis, 'Identity Theft: Assessing Offenders' Strategies and Perception of Risk, Technical Report for the National Institute' NCJRS219122 NIJ Grant No.2005-IJ-CX-0012. 2007, 1-88 available at <http://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf> accessed on 9 May 2011

[20] S Allison, A M Schuck and K M Lersh, 'Exploring the Crime of Identity Theft: Prevalence, Clearance and Victim /Offender Characteristics' (2005) Vol. 33 (2005) Journal of Criminal Justice 19-29

[21] N Robison, H Graux, D M Prrilli, A Klautzer and L Valeri, 'Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report,' 2011, 15 available at <http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf> accessed on 24 Jun. 2013

2.1.2.2.1 Definition of Identity Theft under United States' Criminal Laws:

In the section 1028 of the Identity Theft and Assumption Deterrence Act of 1998, the US legislature defines IT as:

> (a) Whoever, in a circumstance described in subsection (c) of this section:
> 7. knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.[22]

This definition seems to be more comprehensive than many other definitions; however, it is considered by some researchers to be too broad,[23] because it contains some acts, such as credit card fraud and account hijacking that are considered types of fraud, but under this definition they are considered as parts of an identity theft crime.

In addition, it seems that the US legislature does not criminalise the real offence of identity theft because identity theft offence committed before the transfer of or the use of another person's means of identification to commit other illegal activities that are considered a violation of federal law or it constitutes a felony under any applicable State or local law. The using of or transferring of a means of identification is considered subsequent unlawful activities to commit other crimes, such as fraud.

Continuing with U.S laws in its definition of identity theft, the US legislators in section 111 of the Fair and Accurate Credit Transactions Act define identity theft as 'a fraud committed using the identifying information of another person.'[24]

With respect to United States courts perspective, it seems that United States Court of Appeals has adopted the definition that is stipulated in the Identity Theft and Assumption Deterrence Act of 1998, but it has extended it to encompass some acts,

---

[22] S7 (1) Identity Theft and Assumption Deterrence Act of 1998**,** Pub. L. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998), *codified at* 18 U.S.C. §1028.

[23] N Meulen, 'The Challenge of Countering Identity Theft: Recent Developments in the U.S., the U.K, and the E.U, International Victimology Institute Tilburg. September' (2006) 2 available at <http://www.samentegencybercrime.nl/UserFiles/File/Rapport%20identiteitsfraude%20universiteit%20tilburg.pdf> accessed on May 25, 2011

[24] S 111 of the Fair and Accurate Credit Transactions (FACT) Act of 2003 (FACT Act), Pub. L. No. 108-159, 117 Stat. 1952 (Dec. 4, 2003)

such as counterfeiting individuals' signature. In *United States v. Blixt*[25] for instance, the court considered the signature of an individual as a means of identification and using it without consent constitutes identity theft. It might be said that this expansion is unnecessary because this unlawful act may be governed by other legal materials, such as forgery provisions.

2.1.2.2.2 Identity Theft Definition in Canada Legislation:

In contrast to the USA legislation, the Canadian legislature defines identity theft in s4 of the Canadian Bill 2009, which amended the existing Criminal Code (identity theft and related misconduct). In this section, it has been stated that identity theft is knowingly obtaining or possessing "another person's identity information in circumstances giving rise to a reasonable inference that the information is intend to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence".[26] In addition, it is mentioned that a person may commit an offence if he transmits, makes available, distributes, sells, or offers for sale another person's identity information. It is also an offence if he has it in his possession for any of those purposes, knowing or being reckless that or as whether the information will be used to commit an indictable offence that include fraud, deceit or falsehood as an element of offence.[27]

The Canadian legislature creates two offences of identity theft: (1) unlawful obtaining or possession and (2) trafficking in personal information of other persons. Moreover, it refers to the state of recklessness and considers it as an element of *mens rea* of the identity theft offence. From the above definition, it seems that the Canadian legislature criminalises the factual commissioning of identity theft. It criminalises the obtaining and possession of another person's identity. Therefore, it mentions some criminal activities, such as counterfeit credit or debit cards, losses due to lost or stolen credit cards or some of the fraud activities as a result of identity theft.[28]

[25] *United States v. Blixt*, 548 F. 3d 882 C.A.9 (Mont.), 2008

[26] Bill s 4 Act amended Identity Theft and Related Misconduct 404, 2(1) Canada 2009 available at <http://www.cba.ca/contents/files/submissions/sub_20090603_01_en.pdf> accessed on 25 May 2011

[27] ibid section 2(2)

[28] ibid

2.1.2.2 .3 Definition of Identity Theft in Australia Legislation:

In Australia, identity theft is not a federal crime. As a result, each State of the five Australia States has its own legislation. For example, the South Australian legislature considers the use of another person's information to commit an illegal purpose as identity theft. It defines it as:

> A person who makes use of another person's personal identification information intending, by doing so to commit or facilitate the commission of, a serious criminal offences is guilty of an offence and liable to the penalty appropriate to an attempt to commit the serious criminal offence. [29]

The Queensland legislature also considers the obtaining or the use of another person's means of identification with intent to commit other crimes as identity theft. Thus, it defines identity theft as:

> A person who obtains or deals with another entity's identifying information for the purpose of committing, or facilitating the commission of an indictable offence commits a misdemeanour.[30]

In addition, the Queensland legislature makes the possession of another person's information or the use of this information as a crime.[31]

The Victoria legislature creates two types of identity theft: (1) making, using, supplying and (2) the possession of another person's means of identification with intent to commit another crime(s). The Victoria legislature, for instance, in sections 192B and 192C states that a person is guilty of an offence if he commits one of the instances that are stated in theses sections. It in section 192B (1) considers a person is guilty of identity theft if he 'makes, uses or supplies identification information (that is not identification information that relates to that person'.[32] In addition, it in section 192C (1) considers a person, who 'possesses identification information (that is not identification information that relates to the person)' is guilty of identity theft.[33]

Contrast to Queensland legislation and South Australia legislation Victoria legislation

[29] South Australia Criminal Law Consolidate Act of 1935 s 144C amended in 2003
[30] Queensland Criminal Act of 1899 s 408D ins 2007 No. 14 s16 and amended in 2010 s 1 (4)
[31] Queensland Criminal Act of 1899 S 408D sub. 7
[32] Victoria's Crimes Amendment Act 2009 section 192B No.22 of 2009
[33] ibid section 192C

does not consider the use of identification information of another person with his consent an offence. However, Victoria legislation considers the possession of identification information of another person an offence even if the crime that s/he intends to commit is an impossible crime.[34]

The New South Wales legislature considers dealing with identification information of another person with intent to commit an offence as a crime. It in section 192J states that '[a] person who deals in identification information with the intention of committing, or of facilitating the commission of an indictable offence is guilty of an offence.[35]

In addition, the New South Wales legislature considers the possession identification information of another person as a crime. It is stated in section 192K that '[a] person who possesses identification information with the intention of committing, or of facilitating the commission of, an indictable offence is guilty of an offence'. [36]

Similar to Victoria legislation New South Wales legislation considers the possession of identification information of another person with intention to commit an offence as a crime even if the crime that is intended to be committed is an impossible crime.[37]

Like other Australia States, the Western Australian legislature considers the use of another person's means of identification to commit other crimes as a crime.[38] The Western Australian legislature also considers the possession of another person's means of identification with intention to commit an offence as a crime. [39]

2.1.2.2.4 Definition of Identity Theft in the UK Legislation:

In contrast to those countries examined above, under United Kingdom law there is no clear cut definition for the identity theft. As well, the theft provisions in the Theft Act 1968 do not directly refer to the unlawful use of another person's means of identification without his consent. In addition, the British courts do not define it. They

[34] Victoria's Crimes Amendment Act 2009, supra note, 32, section 192D (2)
[35] New South Wales's Crimes Amendment (Fraud, Identity and Forgery Offences) Bill 2009 section 192J
[36] ibid section192K
[37] ibid section 192M
[38] Western Australia Criminal Code Amendment (Identity Crime) Act 2010 (No. 16 of 2010), section 490
[39] ibid section 491

do not consider the act of the unlawful obtaining of another person's means of identification as a crime. In their reasoning the courts pointed out that this means of identification is intangible, and the intangible thing cannot be subject to theft. In *Oxford v. Moss*,[40] which occurred in Liverpool University in 1979, the court refused to consider the appropriation of exam information that was taken from the University as theft with the application of the Theft Act 1968. The court reasoned its decision that the information, which was taken, was unsuitable to be considered a stolen subject. Therefore, the court acquitted the perpetrator.

Even though the UK legislature in the Fraud Act 2006 implicitly has considered the unlawful use of personal information as a crime, it does not define identity theft. With respect to this unclear situation of the UK legislature, one may believe that the Fraud Act 2006 has consolidated the two concepts: identity theft and identity fraud and called them identity fraud.

However, the United Kingdom Home Office, currently, defines identity theft as an activity that 'occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual the victim is alive or dead'.[41] The cabinet office in its report that issued in 2002 did not define identity theft, but it stated that identity theft considered 'a harrowing experience for individuals whose identity is taken or stolen', and it is associated with the organised crime. Additionally, the cabinet office stated that identity theft is not a crime in itself. Consequently, the legislature should create a new crime of identity theft.[42]

The UK legislation, contrast to the Federal Identity Theft and Assumption Deterrence Act of 1998 does not separate between the use of a real person's means of identification and the false means of identification to commit other crimes. The UK legislature brands the use of the means of identification as identity fraud, whereas the US legislature brands the transfer of or the use of another person's means of identification as an identity theft offence, and the use of a false identity or giving false information to gain

[40] *Oxford v Moss* [1979] Crim LR 119 DIVQBD

[41] Home Office, 'Identity Crime Definitions' 2006 available at <http://www.identity-theft.org.uk/definition.html> accessed on 26 May 2011

[42] Cabinet Office, 'Identity Fraud: A Study' 2002, 3-5 available at <http://www.statewatch.org/news/2004/may/id-fraud-report.pdf> accessed on 19 July 2011

benefit as identity fraud.

Evidently, one could argue that there is no universal definition of identity theft. It seems that some countries move ahead to conceptualise and incorporate it in their statutes, while some others have failed to make adequate provisions for it. This does not actually mean that identity theft is not captured in their legal codes.

The difference between academic scholars and legislators in legislation of other jurisdictions about the identity theft definition may give other researchers an opportunity to establish a workable definition for identity theft.[43] Therefore, the author defines identity theft as: a person is guilty of identity theft if he 'knowingly and willingly or recklessly and dishonestly, without consent obtains by any method whether sophisticated or not, personal or financial information of another person whether a legal entity or an individual person, transfers, sells, offers for sale, distributes, makes the use of this information available for others or uses this information for their own purposes. In essence, what are the features of IT and how does it differ from other forms of crime? In the next section, the characteristics of identity theft will be explored and discussed.

2.2 Features of Identity Theft:

Drawing from the above various definitions proposed by various legislation and scholars, the following features of identity theft can be drawn.

2.2.1 Identity Theft Is a Non-Violent Crime:

Such a crime usually requires careful planning and a high level of intelligence to obtain another person's means of identification. Therefore, the criminal sometimes use sophisticated methods, such as phishing to deceive and persuade the victim into divulging his personal or financial information to him. There is no violent can be used by the criminal to obtain this information. After the criminal has obtained another person's means of identification, he uses it to commit other crimes, such as open a new account in a victim's name or perpetuate his existing account. As a result, identity theft sometimes called a financial crime or a means to commit financial crimes.

[43] N Meulen, supra, note 23

2.2.2 Identity Theft Cannot to Be Discovered Easily

Identity theft can be more difficult to detect and identify because it often takes a long time before it is discovered, particularly offline identity theft, such as stealing another's identity to avoid a possible arrest by the police or carry out other unlawful activities relate to non-credit cards. In addition, stealing a child's identity and then using it to commit other crimes may not be discovered until the child becomes an adult or applies for a driving license. Identity theft sometimes takes a period of time that can range from 6 months to several years to be discovered,[44] because discovering identity theft depends occasionally on the amount of the loss that the victim may suffer.[45] It also depends on some activities that victims may accomplish, such as applying to obtain financial benefits for example loans, mortgages or applying for driving license. Moreover, identity theft may take a long time to be discovered because the victim sometimes does not report his victimisation to the police.

2.2.3 Identity Theft Is Difficult to Be Proved:

Occasionally, identity theft is carried out over the internet remotely. As mentioned above, it may take a long time to be discovered. As a result, there are some difficulties may be faced when the commission of identity theft is proved by the law enforcement agency or the court. Identity theft may be committed, for instance, from the state territory, which does not consider the use of another person's means of identification as crime. In this case, it is difficult to get cooperation between the State that the crime has been committed from its territories and the State that the crime is committed on its territories. In addition, if identity theft is committed correctly it is impossible to be tracked because the perpetrators have the ability to conceal their crime. They may remove all the evidence from the crime scene, as well as, conceal their own identity. Victims sometimes contribute to these difficulties when they do not report their

---

[44] Identity Theft Resource Centre, 'Identity Theft: The Aftermath 2003
A Comprehensive Study to Understand the Impact of Identity Theft on Known Victims' 4 available at <http://www.idtheftcenter.org/artman2/uploads/1/The_Aftermath_2003.pdf> accessed on 22 May 2011
; J Benner, et al, 'Nowhere to Turn: Victims Speak Out on Identity Theft ACalpirg/ PRC Report' 2000, 2 available at <http://www.popcenter.org/problems/credit_card_fraud/PDFs/identity%20CALPYRG.pdf> accessed on 22 May 2011

[45] G Newman and M McNally, 'Identity Theft Literature Review' 2005, 6 available at <http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf > accessed on 9 May 2011

victimisation to the police.

2.2.4 Cross – Jurisdictional and Cross-National:

People always use the internet to accomplish their transactions. The internet is used to connect the world States. It has become a truly trans-national medium. Therefore, information about individuals, such as their social security numbers, names, PIN numbers or driving license numbers has become available everywhere. As a result, perpetrators can easily obtain the personal information of any person that they want from anywhere.[46]

Identity theft may take place from any region or country in many regions or countries. It can remotely be committed from within one country against another country externally. Consequently, identity thieves may be subject to more than one jurisdiction because each country has its own legislation that governs identity theft. This may lead to a conflict among jurisdictions.[47] A conflict of jurisdictions may require determining which one of these jurisdictions has the authority and responsibility to investigate identity theft and prosecute criminals.

This feature of identity theft offence requires global cooperation to combat identity theft. It also requires activation the extradition treaties to help law enforcement efforts to catch the perpetrators and prosecute them.

2.2.5 Identity Theft Has Many Sequences Activities:

When most perpetrators decide to commit identity theft they may do many activities, such as determining another person's information, determining the way in which they can steal this information, and then carry out the crime, and how can they use this information to obtain financial benefits or any other benefits. These sequence activities may make more than one perpetrator involved in the commission of identity theft. This may give rise to the criminal participation issue in committing identity theft offence.

As stated above, most of the activities that lead to the commission of identity theft may

---

[46] K M Saunders and B Zucker, 'Counteracting Identity Fraud in the Information Age: the Identity Theft and Assumption Deterrence Act' (1999) Vol. 8 Cornel Journal of Law and Public Policy 661-675

[47] G Newman and M McNally, supra, note 45, 7

happen in many regions or many countries. Consequently, investigation, extradition and prosecution in identity theft cases may be very difficult. In addition, it may lead to conflict among the laws to choose the law that can be used, as well as the court, which has jurisdiction to prosecute the perpetrator. A conflict among laws and jurisdictions may lead to find no law that can be applied to prosecute the perpetrator because the crime may not be committed in a specific State or it may be committed in a State does not criminalise the taking of another person's identification without consent. This feature may be considered a subset of the previous feature.

2.2.6 Strong Nexus between Identity Theft and Cybercrimes:

As mentioned previously, the internet has become an indispensable tool in people's life. It is used to accomplish numerous transactions. In addition, individuals can use it to achieve their transactions from anywhere in the world. However, as the internet has become a means to accomplish commercial transactions, identity theft criminals as well developed their methods to commit identity theft by using it.

Criminals sometimes use sophisticated methods that relate to internet, such as phishing, Trojan Horse, viruses and spyware to commit identity theft. As a result, some scholars believe that identity theft is primarily a result of internet and the information age.[48] It could be said that the internet is considered the first reason that facilitates the commission of this crime in our lives.

2.2.7 Identity Theft Is the Fastest Growing Crime in the World:

Identity theft is the one of the fastest growing crimes in the world because it takes little time to be committed, particularly online identity theft. It can be committed at a high speed. It has rapidly growth and aggravated criminal activities. It can attack a huge number of victims in the same time.

Each year, crimes that are committed by using stolen identities cost individuals, governments, and financial institutions a great loss in both their financial and their reputations. For instance, more than 700,000 American fall victims of identity theft

[48] G Newman and M McNally, supra, note, 45, 7

every year.[49] In addition, they cost the UK's economy almost £1.7 billion per year.[50]

2.2.8 Identity Theft: One Model, Many Faces:

Perpetrators may commit identity theft in different ways for different purposes. In addition, they may commit it to facilitate other crimes, such as fraud that is committed against the victim's finances or to avoid police arrest.[51] Perpetrators may steal, for example, the personal information of people, such as their names or addresses to commit credit card fraud, open a new account in their names or any other crimes that can be committed against the victim's finances. On the other hand, they may steal this information to use it to commit crimes against the victim himself. Crimes that are committed against the victim by using his stolen identity can be imagined when the criminal gives this stolen identity to the police to avoid the arrest, and then he disappears after he is released. As a result, the victim may be persecuted because he field to attend the trial of crimes that have been committed by using his identity.

As a consequence of the above crimes, victims suffer two types of effects: (1) Financial effects that occur when the perpetrator uses the victim's identity to open a new account in his name and (2) criminal effects, which occur when the perpetrator uses another person's information to avoid arrest or an arrest warrant for another crime. The multi-faceted nature of identity theft has created difficulty to give sufficient definition to it[52] and so, it cannot be determined accurately.

---

[49] S R Cherry, 'Al-Qaeda May Be Stealing Your ID, Insight on the News' Aug. 26, 2002 at 18 available at <http://findarticles.com/p/articles/mi_m1571/is_31_18/ai_90990420/pg_2/?tag=mantle_skin;content> accessed on 25 May 2011; A Brooke Masters and E Caroline, Mayer, 'Identity Theft More Often an Inside Job, Newsbytes News Network' Dec. 3, 2002 cited in E L Sylvester, 'Identity Theft: Are the Elderly Targeted' (2004) Vol. 3 (2) Connecticut Public Interest Law Journal; in last study that has been done by the Federal Trade Commission referred to that 3.25 million Americans have been victimization of identity theft. U.S. Department of Justice, available at <http://www.usdoj.gov/usao/mt/identity_theft/.> accessed on 20 May 2011; R Parisi, 'Identity Theft: A Fast Growing Problem' (2007) Vol. 2 (1) Risk Intelligence 1-2

[50] According to Report Published in February 2006 by UK Home Office. Available at <http://www.identitytheft.org.uk/cms/assets/Cost_of_Identity_Fraud_to_the_UK_Economy_2006-07.pdf> accessed on 9 May 2011

[51] N Van der Meulen, supra, note 23, 5

[52] N Meulen and B J Koops, 'The Challenge of Identity Theft in Multi-level Governance Towards a Co-Ordinated Action Plan for Protection and Empowering Victims' 2009, 3 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1447324> accessed on 27 May 2011

2.2.9 Identity Theft Has Constant Effects against the Same Victim:

Repeated the use of the stolen identity means an offender uses the person's identity more than one time to generate money or opportunities for other crimes. In addition, he may repeat using the person's identity many times until the identity become useless.[53] The identity thief often uses another person's means of identification to involve in a series of fraudulent exercises.[54]

2.3 Distinction between Identity Theft and Other Forms of Crime:

Identity theft is a crime relating to the internet and modern technology. It also relates to finance and property of an individual. Therefore, similarity and differences may be found between identity theft and other crimes, such as identity fraud and identity crimes. It is suitable here to distinguish identity theft from these crimes as mentioned below:

2.3.1 Differences between Identity Theft and Identity Fraud:

Several differences exist between identity theft and identity fraud. These distinctions would be explained in bits.

2.3.1.1 Differences in Terms of Conceptualisation:

Identity theft is a crime that occurs when a person knowingly transfers or uses, without lawful authority, a means of identification of another's person with intent to commit, or to aid or abet, any unlawful activity,[55] while identity fraud is a crime occurs when the perpetrator uses a false identity to obtain the victim's property. In other words, identity theft occurs when the person takes a real person's means of identification, such as her social security number, PIN or her password without her consent, while identity fraud occurs when the perpetrator obtains financial benefits from the victim with her consent

[53] G Newman and M McNally, supra, note 45, 5

[54] U.S. Department of Justice, 'Identity Theft, Problem-Oriented Guides for Police, Problem-Specific Guides Series' No. 25 (June 2004) at 1 available at <http://www.cops.usdoj.gov/mime/open.pdf?Item=1271 > accessed on 27 May 2011

[55] Identity Theft Act and Assumption Deterrence Act of 1998 §1028

by using a false identity.[56]

2.3.1.2 The Way in Which the Defendant Takes the Property:

Identity theft occurs when the perpetrator directly or indirectly takes personal information of another person from him without his permission, while in identity fraud the perpetrator takes the property from the victim by the cheating or dishonesty. In addition, the perpetrator of the identity fraud offence sometimes creates a new identity by using facilities, such as a copy identity device. In the identity fraud crime, the criminal does not steal the means of identification, while in the identity theft crime, he steals the individual's means of identification, and then uses it to create a new category of victim.[57]

2.3.1.3 Scope of the Crime:

Identity theft occurs when the perpetrator falsely represents himself as another actual person to accomplish illegal actions. In other words, identity theft contains the use of the real person's identity only, while identity fraud contains both the using of the actual individual and the using of an untrue identity.[58] The using of the fictitious and true identity to commit identity fraud means that the identity fraud offence is broader than identity theft offence.[59] As a result, this encourages some researchers to believe that identity theft is a subset of identity fraud.[60]

2.3.2 Distinguishing between Identity Theft and Identity Crime:

An identity crime is a crime broader than identity theft. The identity crime may contain both identity theft and identity fraud.[61]

---

[56] G Newman and M McNally, supra, note 45, 1

[57] G Newman and M McNally, supra, note 45, 1

[58] D Lacey and S Cuganesan, 'The Role of Organizations in Identity Theft Response: The Organization-Individual Dynamic' (2004) Vol.38 (2) the Journal of Consumer Affairs 244-261

[59] G R Gordon and N.A, Willox, 'Identity Fraud: A Critical National and Global Threat' (2004) Vol. 2 (1) Journal of Economic Crime Management 7

[60] D Lacey and S Cuganesan, supra, note 58, 245

[61] S Susan and A Norm, 'Defining Identity Theft- A Discussion Paper' (2006) McMaster business Research Centre McMaster University 9 available at <http://www.business.mcmaster.ca/idtdefinition/IDT%20Discussion%20Paper%20Revision%20from%20Sue%20Sproule%20April%206%2006.pdf> accessed on 9 May 2011

2.3.3 Distinguishing between Identity Theft and Theft:

Both identity theft and theft are crimes committed against individuals' properties. However, identity theft differs from theft because identity theft is a crime that is committed against a specific type of the individuals' properties: intangible property, and particularly the individuals' means of identification. For instance, a criminal may steal other persons' names, their addresses, social security numbers, PIN numbers, mothers' maiden names or their national insurance security numbers, while theft is a crime committed against all individuals' properties irrespective of whether it is tangible or intangible, such as taking their cars or carrying their cheques in action away.

In addition, victims of conventional theft may suffer loss their possessions, but in the identity theft offence, victims lose nothing. Victims of identity theft, however, may suffer damage to their reputation and their status in society. Besides, they may suffer damage that may attack their commercial credit.[62]

Identity theft is a crime, which may be committed to facilitate other crimes (such as fraud, terrorism or to avoid a criminal record) while theft is a crime, which can be committed alone without depending on other crimes. More so, theft offence is broader than identity theft offence. As a result, identity theft is considered a type of theft or a subset of traditional theft. However, as it will be seen, identity theft does not fall within the scope of traditional theft offence and it needs a specific Act to govern it.

2.3.4 Two Main Guises of Identity Theft: Offline and Online:

Both on and offline are typology of identity theft. However, online identity theft occurs when a perpetrator uses a sophisticated virtual technique(s) to obtain a means of identification of another person. A good example of virtual method is the use of software device, such as spam or virus to obtain a means of identification of another person while offline identity theft occurs when a perpetrator openly or physically steals a means of identification from the victim. Often the means of identification is stored in wallets, purses, mailboxes, or bags. Therefore, criminals steal people's wallets or purses to gain their information.

[62] B Diedrich, 'Chapter 254: Closing the Loopholes on Identity Theft, But at What Cost?' (2002) Vol. 34 McGeorge Law Review 383-390

Another state that one can in which find distinguishing between off and online identity theft is offline identity theft is difficult to be discovered and detected while online identity theft, although the perpetrator has the ability to conceal his crime, it can be discovered and allocated easier. Furthermore, potential evidence of online identity theft remains for a short period and then disappears. The evidence of this may, for instance, disappear by merely a simple click by the victim on any key of his laptop or computer. In addition, an offline identity theft offence is older than the online identity theft. It is the first type of identity theft.

2.3.5 Identity Theft and a White Collar Crime:

A white collar crime is a crime that relates to the economy,[63] and it is committed without violence.[64] However, its effects are often diffusing and its victims may be indefinite.[65] It may target both rich and poor people. In addition, victims of the white collar occasionally are stores, banks, or businesses. Sanctions that may apply to white collar crimes may be serious because they can affect the State economy.

Moreover, white collar crimes are considered a breach of trust that the victim has placed with the perpetrator. White collar crimes also contain most crimes that are committed without violence (such as fraud, embezzlement, forgery and all crimes that relate to credit cards, such as theft of a credit card or fraudulent transferring or receiving a credit card). Identity theft as other crimes may be committed to facilitate crimes that relate to economic, such as fraud. In addition, it may be committed without violence. As a result, it is considered a type of white collar crimes. [66]

In nutshell, identity theft appears to be a dynamic kind of crime that could be committed on and offline. Besides, it has been argued that identity theft differs from other forms of crime because it not only has two core elements, but the act can also be repeated and employed as a precipitator or catalyst in committing other crime(s). In the next section the typology of identity theft and how each type directly or indirectly can

[63] DPS, Law Enforcement Academy, Santa Fe, New Mexico, 'Criminal Law: White Collar Crimes Online' "without year" available at <http://www.dps.nm.org/trainig/legal/documents/White_Collar_Crime.pdf> accessed on 21 May 2011

[64] S P Green, 'Moral Ambiguity in White Collar Criminal Law' (2004) Vol. 18 Notre Dame Journal of Law Ethics and Public policy 501-519

[65] ibid

[66] DPS, Law Enforcement Academy, Santa Fe, supra, note 63

affect both the perpetrator and the victim will be examined.

2.4 Typology of Identity Theft:

There are many types of identity theft, however, the most frequently mentioned in scholarly and legal profession are online, offline, organisational and non-organisational identity theft. This section intends to explore and discuss different forms or types of identity theft.

2.4.1 Total Deprivation of Victim's Property:

There are two types of identity theft: zero-sum and non-zero phenomenon.

2.4.2 Zero-Sum Phenomenon:

In this type of identity theft offence, the perpetrator completely deprives the victim of his means of identification, and then uses it to derive benefit(s) for himself or for others. The criminal uses total or most of the victim's means of identification.

2.4.3 Non Zero-Sum, Online Versions:

This type of identity theft offence means that the perpetrator uses some of the victim's means of identification. He does not completely deprive the victim of his means of identifications; he may make a copy for them and leaves the original with him.[67]

2.4.4 On and Offline Identity Theft:

As mentioned previously, identity theft can be committed on and offline. Therefore, it consists of two types: on and offline identity theft. Offline identity theft occurs when a perpetrator uses traditional or physical methods, such as stealing a wallet or a purse, stealing mailbox contents or dumpster diving to obtain another person's means of identification.[68] It is the first and old type of identity theft. It is used to commit other

[67] M CHawki and M Abdel Wahab, 'Identity Theft in Cyberspace: Issues and Solutions' (2006) Vo. 11 (1) Lix Electronic, Printemps 1-41

[68] OECD, Organization for Economic Co-operation and Development, 'OECD Policy Guidance on Online Identity Theft' 2008, 2 available at <http://www.oecd.org/dataoecd/49/39/40879136.pdf > accessed on 5 July 2011

crimes before online identity theft can be used for many years.[69] However, the advancement in technology encourages the perpetrator(s) to develop his technology methods to commit identity theft. Nowadays, the perpetrator(s) uses sophisticated methods (such as phishing, malware, viruses and social engineering) to commit identity theft. Identity theft that is committed by using these sophisticated methods is called online identity theft.[70]

Online identity theft is more sophisticated and complex than offline identity theft. As well, online identity theft differs from offline identity theft through the quantity of information that can be obtained.[71] Although in online identity theft the perpetrator(s) uses sophisticated technology to conceal his crime, it can be discovered easy. However, offline identity theft is difficult to be discovered because it depends on monthly bill and the victim may be unaware for the changes that have been taken place in his statement.[72] The perpetrator(s) sometimes uses the victim's name for a long time and many times before he discovers the unlawful use of his/her name. Consequently, the only domestic criminal law of the State relates to identity theft is insufficient to combat identity theft. Combating and preventing this form of crime needs cooperation between all parties.[73]

In spite of online identity theft is a widespread crime and it a new crime relates to cyberspace, but the commission of offline identity theft still takes place more than the

---

[69] L Bell, 'Offline Identity Theft-Not All Theft Happens Online' 2007 available at <http://ezinearticles.com/?Offline-Identity-Theft---Not-All-Identity-Theft-Happens-Online&id=5862168> accessed on 6 July 2011

[70] OECD, Organization for Economic Co-operation and Development, supra, note 68, 3

[71] Better Business Bureau, 'New Research Shows That Identity Theft is More Prevalent Offline Than Online, Press' January 26, 2005 available at <http://www.bbb.org/us/article/new-research-shows-that-identity-theft-is-more-prevalent-offline-with-paper-than-online-519> accessed on 6 July 2011

[72] U.S. Department of Justice, National Institute of Justice, 'Identity Theft-A Research Review' 2007, available at <https://www.ncjrs.gov/pdffiles1/nij/218778.pdf> accessed on 7 May 2011

[73] M J Elston and S A Stein, 'International Cooperation in On-Line Identity Theft Investigations: A Hopeful Future but a Frustrating Present': a paper submitted at the 16th International Conference of the International Society for the Reform of Criminal Law held at Charleston, SC, USA from December 6 - 10 ,2002, 21 available at <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf> accessed on 4 July 2011; ISPAC, 'The Evolving Challenge of identity-Related Crime: Addressing Fraud and the Criminal Misuse and Falsification of Identity' Edited by D Chryssike, N Passas and Ch D Ram, 2008 available at <http://www.ispac-italy.org/pubs/ISPAC%20-%20Identity%20Theft.pdf> accessed on 6 July 2011; Emigh A and Labs R, 'Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures' 2005 available at <http://www.antiphishing.org/Phishing-dhs-report.pdf> accessed on 5 July 2011

commission of online identity theft.[74] Both off and online identity theft may be committed by one individual criminal or many individual criminals with or without an agreement between them. In addition, they may be committed by perpetrators who join with each other in regular or irregular groups. This may lead to new types of identity theft. The next section will give an idea about each type.

2.4.5 Organisational and Non-Organisation Identity Theft:

Identity theft may be committed by one or more than one person without an agreement between them. However, it may be committed by an organised or a regular group, such as network rings.

2.4.5.1 Non-Organisation Identity Theft:

A non-organisation or irregular identity theft or traditional identity theft offence means an identity theft offence is committed by one perpetrator or more than one perpetrator without an agreement between them. In *United States v. Godin*[75] that happened in 2006, the perpetrator could, for example, defraud eight banks and credit unions and got almost $40,000, by using another actual person's identity and other false identities with a fabricated social security number.

In addition, identity theft may be committed by perpetrators under their consensus, but without an agreement. For instance, a perpetrator(s) intends to commit identity theft and he begins to gather information about individuals. Meanwhile, another perpetrator(s) may know his intention to commit identity theft and decide to help him. Both the perpetrator who intends to commit identity theft and the perpetrator who helps him may be guilty of identity theft.

The above provisions are governed by criminal public rules. These rules draw the methods that a crime can be committed with and the participation in crimes.[76] It was

---

[74] Better Business Bureau, supra, note 71; S Seljan et al, 'E-Identity: Responsibility or Commodity' 2007 available at <http://infoz.ffzg.hr/INFuture/2007/pdf/3-05%20Seljan,%20Stancic,%20Crnec,%20Salopek,%20E-identity.pdf> accessed on 6 July 2011

[75] *United States v. Godin* 534 F. 3d 51; 2008 U.S. App. Lexis 15301; J N Woodworth, 'Case Comments' (2009) Vol. XLII Suffolk University Law Review 1013- 120

[76] See sections 47, 48 of the Iraqi Penal Code No. 111, 1969; section 8 of the Accessories and Abettors Act 1861, c. 94 (UK)

mentioned in these rules that a crime can be committed by one person or more than one person. Therefore, an identity theft perpetrator can alone commit IT or another perpetrator(s) may aid or abet him or her.

A perpetrator(s) who commits an element of the *actus reus* of identity theft is called a principal perpetrator[77] whereas he is called a secondary participator if he does not commit an element of the *actus reus*,[78] but he aides or abets in the commissioning of identity theft.[79]

Identity thieves may make an agreement among them to commit identity theft and carry on to accomplish it. This agreement is called a criminal enterprise. The crime that is committed according to this criminal enterprise is called an organisation identity theft offence and the groups that commit it are called organisation rings.

2.4.5.2 Organisation Identity Theft:

Identity theft may also be committed by individuals or organised groups. Identity theft that is committed by organised groups is called an organised identity theft offence. Organised groups are defined as two or more than two people who make an agreement between them, typically to commit a crime.[80] Perpetrators sometimes need to join with other perpetrators to commit identity theft because it has more than one action and it requires more than one person to carry out it. As a result, a perpetrator(s) may hold an agreement with another perpetrator(s) or enter a criminal enterprise to obtain another person's means of identification that he wants, and then uses to commit other crimes.[81]

An organised identity theft offence frequently takes place in credit card fraud.[82] Offenders may use a high technology to commit an organised identity theft offence and to avoid recognition. In 2008, for instance, a perpetrator and his girlfriend stole another person's driving license, and then used the victim's name and date birth that were found

[77] C Elliot & F Quinn, *Criminal Law* (8th edn Pearson Longman London 2010) 282

[78] A Ashworth, *Principles of Criminal Law* (6th Oxford University Press United States 2009) 407

[79] S Wilkins, 'Criminal Law-Accomplice Liability' (2007) Vol. 85 University of Detroit Mercy Law Review 69-73 (70); C Elliot & F Quinn, supra, note 77, 283; A Ashworth, ibid, 404

[80] C Elliot & F Quinn, supra, note 77, 262

[81] *United States of America v. Landy Diaz*, (4th Cir. 2011) No. 10-4305 unreported; J D Ohlin, 'Joint Intentions to Commit International Crimes' 2010, 3 available at <http://www.law.upenn.edu/academics/institutes/ilp/2010papers/OhlinJointIntentionsInternationalCrimes.pdf > accessed on 6 July 2011

[82] G Newman and M McNally, supra, note 45, 5

in to make a false credit card. They used software program to make this false credit card. They placed a false address and a perpetrator's picture on it, and then used it to commit other crimes.[83]

However, occasionally, the commission of identity theft does not need cooperation among perpetrators and one person can commit it because it consists of a simple act. This type of identity theft is called individually identity theft or an irregular identity theft. Having examined various types of identity theft, now let us explore the main parties of identity theft.

2.5 Parties of Identity Theft Offence:

Very few researches have been conducted about the parties of identity theft offence. Nevertheless, the knowledge about parties of an identity theft offence would be crucial. Parties of IT comprise of two groups: Victims and perpetrators.

2.5.1 Victims:

Victims of identity theft encompass individuals or firms whose information or services have been stolen[84] and the financial institutions. Drake[85] pointed out that one in fifty of customers suffered identity theft. In addition, he stated that two studies have been conducted and indicated that there are almost 7 million victims annually in the U.S. This means the number of identity theft victims each month is approximately 583,000, and the number each week was almost 135,000, while in each day, the number of victims was approximately 19,000. If one goes further he will find the number of victims is almost 800 in each hour. Moreover, he may find it nearly 13 victims in each minute.[86] Victims of identity theft are divided into two groups: individuals and firms.

2.5.1.1 Individuals as a Victim of Identity Theft:

Despite the individuals' means of identification have been stolen they sometimes do not

[83] *United States of America v. Brown*, (3rd Cir. 2011) No 10-3170 unreported
[84] G Newman and M McNally, supra, note 45, 21
[85] E Drake, *50 Plus One Tips to Preventing Identity Theft* , Encouragement Press, L L C, 1261, W.Glenlake, Chicago IL.60660
[86] ibid, 4

treated as victims of identity theft because they do not incur any financial loss.[87] In addition, identity theft affects companies and creditors rather than them.[88] According to this view, the real victim of identity theft is the companies, which extend the credit to the criminal(s) and the defraud creditors whose goods or services were stolen. It could be said that individuals actually, formally and technologically are classified as a victim of identity theft. More than 9.9 million American, for instance, fall victim to identity theft in 2009.[89]

In effect, every person could be a victim of identity theft. There is no difference between the low and the high rank of people, such as the politicians and states' president.[90] However, there are differences among them according to their exposure to identity theft. Some categories may be at greater risks than other categories. For instance, young adults between the ages of 18-29 represent 52 per cent. While adults between the ages of 30-39 represent the highest category exposure to risks of identity theft because they use the internet in their whole life to make purchases, such as buying an apartment, a house and then furnished it, wedding and the birth date of children.[91] Highly educated groups may also be more susceptible to identity theft risks than less educated groups. The person who is in a high level may be more susceptible to identity theft risks than a person who is in a low level.[92]

2.5.1.2 Identity Theft Targets the Elderly Persons:

Identity theft often spare no vulnerable individuals particularly the aged or elderly persons who are few in enter into independent financial business. Moreover, perpetrators have not targeted them in particularly because they are a defenceless category. Therefore, they represent 10 percent of identity theft victims.[93] However, if the unable individuals fall victim of identity theft they rarely discover immediately that

---

[87] G Newman and M McNally, supra, note 45, 21

[88] L Cradduck and A McCullagh, supra, note 15, 4

[89] C J Hoofnagle, 'Internalizing Identity Theft' (2010) University of California Journal of Law and Technology 1-24 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1585564> accessed on 27 May 2011

[90] G Newman and M McNally supra, note 45, 22

[91] E Drake, supra, note 85, 3

[92] K B Anderson, 'Identity Theft: Does the Risk Vary With Demographics?' (2005) 1-46 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=795427> accessed on 27 May 2011

[93] E Drake, supra, note 85, 3

they become victims of an identity theft offence.[94] In addition, most of people in this category rarely report the identity theft crime that is committed against them[95] to the police.

The identity thief may be known to the aged or elderly people. He may be trusted by the victim. For instance, an unable woman who was suffering from dementia was a victim of identity theft, when her caregivers had stolen her identity and gained approximately $200,000 from her existing account. They also used her information to open a new account. Moreover, they had got funds in her name to purchase new cars for themselves and removed $176,000 in U.S. Savings Bonds from her safe-deposit boxes by using a false lawyer authority.[96]

2.5.1.3 Children as a Victim of Identity Theft:

Even children are not immune and they often fall victim of identity theft. However, there is no sufficient sources of information relates to this category of victims. In addition, it is not commonly available in the public place. Consequently, the allocation crosswise of the victimisation for this huge age category is unidentified. Newman and McNally[97] mentioned that this type of identity theft victims is the largest occurring in the United States. It appears to be an unlimited crime.

It is difficult to determine the stealing of children's means of identity because it cannot be discovered until the children apply for credit, driving licence or after they reach the legal age.[98] In addition, it can be committed by the children's family members (such as their parents, grandfathers, grandmothers, or any other persons who have the power over children's means of identification). Those criminals have also an extreme access to this information. Accordingly, it is difficult to discover this type of identity theft.

---

[94] G Newman and M McNally, supra, note 45, 25; Florida, 'Sixteenth State-wide Grand Jury (Jan. 10, 2002) State-wide Grand Jury Report: Identity Theft in Florida First Report of Sixteenth stat- wide Grand Jury' 3 available at <http://myfloridalegal.com/pages.nsf/4492d797dc0bd92f85256cb80055fb97/758eb848bc624a0385256cca0059f9dd!OpenDocument> accessed on 10 May 2011

[95] Synovate, 'Federal Trade Commission – Identity Theft Survey Report' 12 available at <http://www.ftc.gov/os/2003/09/synovatereport.pdf>accessed on 11 May 2011; G Newman and M McNally supra, note 45, 25

[96] The President's Identity Theft Task Force, supra, note 13, section 10

[97] G Newman and M McNally supra, note 45, 24

[98] ibid 23

2.5.1.4 Deceased as a Victim of Identity Theft:

Effects of identity theft do not restrict to adult persons who are alive, or children, disable or able persons whether ordinary persons or a person who is in a high status. However, they extend to comprise the deceased individuals. In the United States, there is no precise estimate of this type of victim in spite of it being the main purpose to identity thieves for a long time.[99] It was stated that in some instances, certain groups of thieves have stolen nearly 80 deceased's information, such as names, social security numbers, and other credit card information, and then sold it to individuals who were looking for car loans by $600 per name.[100]

Usually, the perpetrator who commits identity theft against deceased individuals, perhaps, is one of deceased family's members, his kin, a person who knows him, or a person who takes care of the patient before his death. It is very easy for the perpetrator to obtain deceased's means of identification by calling the hospital and requiring information about the deceased. In addition, perpetrators may obtain the deceased's information from the press when the deceased family places it as an obituary, death and funeral notice in a local newspaper. He may also obtain it according to his relationship with the victim, such as friend or co-worker. In a recent case that happened in 1993, for instance, it was mentioned that, the perpetrator (Radovan Karadzic who was a Serbian leader and the world's most wanted men.) took the name of a Serb deceased (Dragan Dabic who was killed in Sarajevo) from a database of missing Serbs. After that, he frequently used it to avoid a trial for war crimes and got a new life as a substitute medicine treatment.[101]

Newman and McNally[102] indicated that stealing the deceased's means of identification

[99] T.L O'Brien, 'Identity Theft Is Epidemic, Can Be Stopped' New York Times (2004, 24 October) Section 3:1, 4, 2004 available at <http://www.nytimes.com/2004/10/24/business/yourmoney/24theft.html> accessed 25 May 2011

[100] D Teague, 'Authorities: Scam Took Ids of Deceased' (2004) MSNBC News available at <http://www.msnbc,msn.com/id/3899283/ns/nightly_news/t/authorities-scam-took-ids-deceased/> accessed on 25 May 2011

[101] Identity Theft 911, 'Exploiting the Dead, Identity Theft 91' (2010) Vol.7 (2) New Sletter February 3 Available at <http://idt911.com/en/KnowledgeCenter/~/media/537D837CD5A44EF1A50AA7C818EB5251.ashx > accessed on 25 May 2011

[102] G Newman and M McNally, supra, note 45, 23

is the largest and most grown in the UK. It is raised from 500 cases in 2001 to 16,000 cases in 2003. However, currently, there is no information or statistics on this group. The victimisation of identity theft offence does not stop at individuals; it may extend to encompass other entities.

2.5.1.5 Members of Institutions as a Second Victim of Identity Theft:

The means of identification that is hold by state institutions, such as military, hospitals, universities and banks is more susceptible to identity theft risks. Institutions more expose to the risks of identity theft than individuals. However, the degree of victimisation differs from group to another. Some groups, such as the military service members, students and others may be more exposed to risks of identity theft than the other groups. In a case that happened in late February 2003, for example, it was stated that a perpetrator entered into a University of the Texas computer system and stole the social security number of 55,000 students' alumni and faculty.[103]

In the US, the greater usage of the social security number among institutions of learning increases the opportunities for getting credit.[104] However, members of the military service are more exposure to risks of identity theft than other groups because they give their mobile numbers, service numbers that may include bank credits, and other kinds of accounts to more than one State and even abroad. More so, military members are sometimes found in positions far away from their family. Due to that, they always use their credit cards, mechanical cashiers, and other remote-access monetary services,[105] and that may make them more susceptible to identity theft.

2.5.1.2 Firms as a Victim of Identity Theft:

A firm means a group of people or money, which is established to achieve special purposes, such as purchasing, selling goods, or collecting money or goods to assist the

[103] A Borrus, 'To Catch An Identity Thief' (March 31, 2003 Business Week) available at <http://www.busniessweek.com/magazine/content/03/b3826071_mz020.htm> accessed on 25 May 2011

[104] ibid

[105] U.S. General Account Office, 'Identity Theft: Greater Awareness and Use of Existing Data Are Needed' Report to the Honorable Sam Johnson, House of Representative, 2002a, 62. Washington, D.C. [G A O-02-766] available at <http://www.consumer.gov/idtheft/reports/gao-do2766.pdf> accessed on 25 May 2011

poor people and so on. Clough and Mango[106] pointed out that in some States legislatures did not consider the wrongfully obtaining information of a company as identity theft in the beginning. However, today, companies and other financial institutions are the main victims of identity theft.

2.5.1.3 Effects of Identity Theft on the Victims' Life:

Identity theft is a dangerous crime. It cripples the victim's life, even if his stolen identity is not used to commit other crimes. However, if his identity that has been stolen is used to commit other crimes she may suffer from various effects, such as financial effects, embarrassment and efforts to clean her credit history, which may take months or several years. In *TRW, Inc. v Andrews*[107] that happened in 1993, the thief, for example, stole the victim personal information, and then used to benefit himself, such as renting an apartment, establishing telephone and electric services. In addition, he attempted to get credit service from five creditors. After that, he used his name and address, but he used the victim's social security number to obtain credit account from the Dillard's Department store. (The Dillard's Department store frequently relies on the report that it receives from the Trans Corporation the main part in this case when it grants the credit account to customers). In this case, the Dillard's department store also depended on that report to grant credit account to the imposter. In 1995, the victim realised that her identity was stolen when she refinanced the mortgage on her house. She was surprised and embarrassed because she became dishonest and not creditworthy and in her economic transactions. In addition, she was forced to leave her job and accept another.

Identity theft has side effects on victims' families and society. If, for instance, a person's means of identification is stolen, and then used to commit other crimes his credit history and his reputation may be contaminated. Victims may also spend a long time and much money to repair their credit history.[108] The contamination of the victim's credit history and his reputation may affect his family and make them feel stressed and uncomfortable in their life. Some family members of identity theft victims may lose

[106] B Clough and P Mango, 'Companies Vulnerable to Identity Theft' (2003) AFP Exchange) Vol.23 (4) cited in G Newman and M McNally, supra, note 45, 27

[107] *TRW, Inc. v Andrews*, 534, United States Supreme Court 19 (2001)

[108] G R Newman and M M McNally, supra, note 45, 45

their job. In addition, they may spend much time to prove to the law enforcements that they were a victim of identity theft. With respect to stealing the deceased's means of identification, his family would suffer from identity theft effects rather than the deceased because he died.[109]

2.5.2 Perpetrators:

The second part of identity theft is perpetrators. There is little information about this part of identity theft. Many reasons may cause this lack in the information: as it is mentioned previously, some victims do not know perpetrators who have stolen their identity. Other victims dislike reporting the theft of their identities to the police. Moreover, identity theft consists of many activities, each one of these activities may occur in different areas or in different States. Consequently, that may lead to a result that the jurisdiction in each region or each State does not have an authority to make investigation into the crime and prove the identity theft quite on the perpetrator. However, the strongest reason is that most perpetrators carry out their crimes from a far distance and may remove any evidence of their criminal activities. The difficulty in determining who the perpetrators are may contribute to the lack or no information about them. Especially, most perpetrators have the ability to hide themselves because they have substance criminal's records, such as substance abuse, narcotic trafficking, robbery and other brutal offences. As a result, the perpetrators remain unknown and the proportion of their arresting represents less than 5 per cent to reported cases.[110]

Identity thieves use two types of methods to obtain personal information of individuals: traditional (such as mail stealing, dumpster diving, wallet or purse stealing and workplace files) and non-traditional or sophisticated methods (such as hacking, phishing, keystroke-logging or spyware malevolent programs).[111] Then, they sell this information to other persons, or may use it to carry out other crimes, such as financial crimes, terrorist operations, or obtaining government benefit.[112]

---

[109] N Meulen and B J Koops, supra, note 52, 5

[110] E Drake, supra, note 85, 4

[111] J S Cheney, 'Identity Theft: Do Definitions Still Matter?' (2005) Discussion Paper Payment Credit Card Centre 11 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=815684> accessed on 26 May 2011

[112] The President's Identity Theft Task Force, supra, note 13, section 10

Generally, there are two types of perpetrators; the first group contains an irregular group (individuals) and the organisations group 'serious groups, such as Hell's Angels and Mara Salvatrucha (MS-13) in United States'.[113] The second group is regular (individuals) or organised groups. This type of perpetrators contains the individuals who are working alone or in pairs.[114]

Some scholars[115] classify perpetrators based on the methods that they use to carry out their crime. They, for instance, classify some perpetrators as being high of experienced technology perpetrators and others weakly experienced technology perpetrators. Perpetrators who have high technologies use sophisticated methods (such as phishing, hacking, and spyware) to carry out identity theft, while the perpetrators who have low experience technologies use non-sophisticated methods (such as wallets stealing which contains individual's information, mailboxes or search in the trash) to find a person's means of identification, and then use it to commit other crimes. Other scholars[116] classify perpetrators according to the motive of carrying out the crime.

2.5.2.1 Individual Perpetrators:

Individual perpetrators may begin with drug addiction or participation in the narcotics potential. Identity theft perpetrators were traditionally or initially perpetrators. One of the core features for those perpetrators is that they are opportunists.[117] According to this feature, identity theft perpetrators are divided into two types and under each type of these types, there are two subtypes as:

---

[113] The President's Identity Theft Task Force, supra, note 13, 13

[114] R Jamieson and G Stephen, 'An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organization Impacts' 2007, 5 available at <http://www.pacis-net.org/file/2007/1271.pdf > accessed on 28 May 2011

[115] D Weisdurd, E Waring and W E F Chayet, *White-Collar Crime and Criminal Careers* 2001 Cambridge UK Cambridge University Press 59; N Meulen and B J Kpoops, supra, note 52, (8)

[116] M Yar, 'Computer Hacking: Just Another Case of Juvenile Delinquency?' (2005) Vo. 44 (4) The Harvard Journal 387-399; C Phue, V Lee, K Smith and R Gayler, 'A Comprehensive Survey of Data Mining-Based Fraud Detection Research' 2005 (2) 1-14 available at <http://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf> accessed on 28 May 2011

[117] J Gayer, 'Policing Privacy: Law Enforcement's Response to Identity Theft' California CALPRIG Education Fund 2003, 13 available at <http://calpirgorg.stage.pubintnet-dev.org/sites/pirg/files/reports/policingprivacy2003.pdf> accessed on 20 May 20011

2.5.2.2 Low-Frequency Perpetrators:

This type of perpetrators is divided into two types.

2.5.2.2.1 Engaging in Criminality:

The type of perpetrators engaging in criminality comprises both parents who steal their children's identity and perpetrators who carry out identity theft to avoid a possible arrest by the police or an arrest warrant for another crime.[118]

2.5.2.2.2 Opportunity Exploiters:

Perpetrators in this type are classified according to their purpose of carrying out a crime. Some perpetrators look for an advantage of carrying out the crime, such as overcoming a fiscal hardship, facing sudden lure, or they may be casual perpetrators.[119] A person, for example, may find a wallet on the street, and then use the owner's information that is found inside it to commit another crime, such as obtaining money by deception.[120]

2.5.2.3 High-Frequency Perpetrators**:**

This type of identity thieves is divided into two types:

2.5.2.3.1 Seeker of Opportunity:

This type of perpetrators may not only look for opportunities to carry out a crime, but they also generate amendable conditions to carry out a specific type of crime.[121] They do not need to use sophisticated methods. This type of perpetrators includes dumpster divers, scanners and the garden–variety thieves.[122]

2.5.2.3.2 Stereotypical Perpetrators:

This category of perpetrators may include all types of identity theft. It particularly, relates to an organisation of crime activities, such as the drug-identity theft correlation.

[118] D Weisburd, E Waring, and E CHayet, supra, note 115, 59
[119] C Phue, V Lee, K Smith and R Gayler, supra, note 116, 2
[120] D Weisburd, E Waring, et al, supra, note 115, 64
[121] R Clarke and M Felson, *Routine Activity and Rational Choice* (London: Transaction Press1993) 4
[122] D Weisburd, E Waring, et al supra, note 115, 78; R Jamieson and G Stephen, supra, note 114, 5

Some scholars[123] believe that all high-frequency perpetrators have varied criminal activities, and their childhood contains difficulties, substance essence misuse, and other troubles.

Individual perpetrators sometimes work in rarely small groups to get individuals' information. They may generate false or fraudulent documents to achieve their purposes. A relationship may be found between the addiction of some drugs or alcohol and the identity theft. For instance, drug or alcohol addicts may be involved in identity theft during burglaries, mail stealing, or purses stealing.[124] They may be used by organised perpetrators to carry out identity theft, such as white–supremacist gangs.[125] Consequently, this type may encompass high identity theft criminals.

2.5.2.2 Gang of Perpetrators and Organisations:

It is observed that there is stable increase in the organisation participation types of criminals in identity theft, such as habitual criminals and professional criminals.[126] There are two types of organised perpetrators: (1) formal organised criminals with hierarchical construction, which is considered a serious type and (2) more loosely-organisation. Formal organised criminals encompass organised gangs that are involved in great crimes and well known to the law enforcement because they have been involved in the crimes for a long time, whereas the more loosely organised encompasses criminals who have little organisation. They sometimes depend on the internet to organise their groups, to communicate with each other, and to organise their identity theft operations to be more effective.[127]

Most criminal gangs are situated in different countries. Some of them use the internet to conduct each other. Other perpetrators use real world means to contact other members.[128] Recently, it has been noted increase in organised criminal groups, especially foreign groups. These groups use computers to carry out their criminal

[123] Weinsburd, Waring, et al, ibid, 83-84
[124] M Yar, supra, note 116, 392
[125] The President's Identity Theft Task Force, supra, note 13, Section: 12
[126] G Newman and M McNally, supra, note 45, 27
[127] ibid 27
[128] The President's Identity theft Task Force, supra, note 13, section 13

activities.[129] In addition, they use a high technology (such as phishing, spyware) to commit their criminal activities and defraud victims into disclosing their personal information. They also use a complex means, such as an internet user to log in the victims' computers.

It was stated that in July 2003, for instance, a Russian computer hacker who was the organiser of a criminal venture hacked into the computer of Financial Services Inc., an internet web hosting and electric banking processing company and stole 11 passwords that were used by USA Financial Services Inc. workers to access the FSI computer network. In addition, he obtained a text file contains roughly 3,500 credit card numbers and FSI customers' credits data. After that, one of his criminal enterprise members threatened FSI that if the FSI did not pay $6000 to their group they would disclose the stolen data to the public. Disclosing the personal data to a third party may create huge damage to their computer system, thus, the FSI under this threat were paid $5,000.[130]

2.5.2.3 Organisations as Perpetrators:

Firms and other organisations, such as credit bureaus and online sites may be directly involved in the commission of identity theft because some of them occasionally, sell persons' means of identification (such as names, social security numbers, or mothers' maiden names) to perpetrators. Online sites may, for example, sell a dozen of bank account balance or social security numbers for little cost.[131]

Legislators in some States allow credit bureaus to release or sell non-credit- related, and consumer-verification information to others. It could be argued that granting permission to credit bureaus to sell the individual's information whether credit or non-credit information to others contains many risks to the individuals and that may lead to facilitate the commission of identity theft offence and make it an uncontrolled problem.

2.6 Factors That Facilitate Identity Theft:

There are many factors may be good opportunities to identity theft offenders. These factors may assist offenders to accomplish their crime. Knowing the factors, which

[129] ibid
[130] The President's Identity theft Task Force, supra, note 13
[131] G Newman and M McNally, supra, note 45, 27

participate in identity theft occurrence and make it a great problem, may help all parties to provide sufficient and effective measures of security and to prevent[132] identity theft.

Some of these factors relate to the relationship between the victim and the perpetrator(s), the victim's awareness or to the internet. Some agencies, companies, or states institutions may also involve in the commission of identity theft. Next sections will illustrate how can these factors facilitate or induce perpetrators to commit IT.

2.6.1 Factors Related to Victims:

There are numerous factors related to victims and they may facilitate the commissioning of identity theft such as:

2.6.1.1 Time, Which Identity Theft Takes It to Be Discovered:

Many individuals do not recognise that they have been become victims of identity theft for a long time. This time may take months or years.[133] The time that a person takes to discover identity theft is highly important. It may increase or decrease the commission of crimes that are committed by using stolen identity. If the time between the commissioning of identity theft and its discovery is short it may help law enforcement to detect perpetrators and obtain evidence against them. However, if the time is too long it may help the perpetrators to conceal the evidence that may help law enforcements to detect and prosecute them. On the other hand, it may encourage the perpetrator to continue to use the stolen identity to commit other crimes.

2.6.1.2 Lack of Awareness:

Insufficient education or victims' lack of knowledge about how identity theft occurs may be a factor that assists in the commissioning of identity theft because individuals rarely discover that they have become victims of an identity theft crime immediately. People should have an idea about the methods that are used to obtain their personal information, particularly sophisticated methods (such as phishing, viruses and worms). Consequently, if they have lack in education and are unaware of these methods they

[132] M CHawki and M Abdel Wahab, supra, note 67, 10

[133] B J Koops and R Leenes, 'ID Theft, ID Fraud/or ID Related Crime. Definitions Matter' (2006) Vol. 30 (9) Datenschutz und Datensicherheit 553-556

may easily divulge their means of identification to perpetrators. Other people do no report their victimisation to the police and that may cause a delay in the investigation or the arrest of perpetrators. The arrest of perpetrators is very important so that it can prevent other offenders from committing identity theft offences.[134] Many states, such as United States and United Kingdom established websites for this purpose to teach people and to raise their awareness about identity theft, methods that are used to commit it, its risks and how they can avoid it.[135]

2.6.1.3 Individuals' Negligence:

Many people are not alert in protecting their personal information,[136] and they often divulge their information online.[137] As a result, their information can easily be stolen by perpetrators. Perpetrators may use any method to obtain people's means of identification, even looking for this means in their trash. If people are unaware of their information and fail to shred their unneeded documents and discard in the waste bins the perpetrators may easily obtain this information, and then used it to commit other crimes. People should also be aware when they use the internet and do not disclose their personal information to any person, particularly the person they do not know him. In addition, they should not respond to any email that they do not know its source.

2.6.2 Factors Related to the Perpetrator:

There are many factors related to the perpetrators and it can assist the commissioning of identity theft, such as:

2.6.2.1 Perpetrators' Ability:

Most offenders can use varied criminal activities to obtain another person's means of identification. They also have a high ability to enter into a specific computer, a common computer, or any website that may be used by people to steal the information that belongs to others. In addition, they can commit their crime from a far distance without

[134] M CHawki and M Abdel Wahab, supra, note 67, 10
[135] J S Cheney, supra, not 111, 17
[136] M CHawki and M Abdel Wahab, supra, note 67, 10
[137] Canadian Internet Policy and Public Interest Clinic (CIPPIC), 'Identity Theft: Introduction and Background' CIPPIC Working Paper No.1 (Identity Theft Series) 2007, 11 available at <http://www.cippic.ca/documents/bulletins/Introduction.pdf> accessed on 1 July 2011

leaving any evidence that may refer to their identity.

2.6.2.2 Degree of Trust Afforded to Perpetrators:

Some perpetrators have a relationship with victims of identity theft offences, such as their parents, brothers or sisters, co-workers, flatmates or their employees.[138] Those persons may exploit this relationship to obtain the victims' private information (such as their dates of birth, social security numbers, PIN numbers, or their drivers' licence numbers) and then use them to commit other crimes. This relationship between victims and perpetrators may also give perpetrators easily access to victims' information without hesitation and without obstacles. The proportion of cases that are committed by criminals who are akin to victims represents nine percent of identity thefts.[139]

2.6.3 Factors Related to the Internet:

Nowadays, individuals, governments, companies and other institutions use the internet to accomplish their transactions. The internet has become the lifeblood that nobody can dispense of it. However, on the other hand, the internet may be used to carry out many illegal activities (such as murder, fraud, terrorism and theft). It is described as a double-edged sword. In addition, it may be blessing and curse on people.[140]

The internet is becoming blessing when it is used to make or achieve many transactions that individuals cannot achieve them offline. It assists people who reside in different countries or have no time to do these transactions offline, to do them online. Besides, it may reduce the dangers that may occur from carrying money in cash with them. However, it considered curse because it plays a more important role to make individuals' information available to the perpetrators. Currently, it is very easy for the perpetrators to obtain information about individuals from the internet. As a result, Hoor[141] believes that identity theft is a crime created by the internet. However, this view

[138] M CHawki and M Abdel Wahab, supra, note 67, 10

[139] Craats and Rennay, *Identity Theft: the Scary New Crime that Targets All of Us* (Toronto: Altitude Publishing, 2005) at 136 cited in Canadian Internet Policy and Public Interest Clinic, supra, note 137

[140] ibid

[141] B Hoor, 'Identity theft: The Crime of the New Millennium' USA Bulletin US Department of Justice' March 2001, 1 available at <http://www.justice.gov/criminal/cybercrime/usamarch2001_3.htm> accessed on 23 May 2011

is inaccurate because identity theft has been existed before the internet age.[142] It is correct; that the internet has made the process of the unlawfully obtaining of personal information much easier,[143] but it does not create the identity theft offence.

Internet service providers may also assist the commission of identity theft or facilitate the opportunity to commit identity theft when they present a manner to educate others about how one can create alternative identities. In this way, they may encourage identity theft offenders to obtain another person's personal information, and then create false identities to commit other crimes.[144]

2.6.4 Credit Reporting Agency and Creditors:

Credited reporting agencies and creditors may involve in the commissioning of identity theft. For instance, every potential lender when he receives a consumer request will hunt for a credit report from a credit reporting agency, which is a personal firm. This credit report agency collects information about consumers and sells reports to potential lenders. The potential lender may undertake the same process every time that the consumer applies for a loan and look for reports from a credit report agency. Consequently, the personal information of the consumer may be found in everywhere.[145] Due to the agency does not allow individual to check the contents of the report,[146] which may be incorrect the potential lender and the credit report agency may facilitate the commission of identity theft because the personal information may fall between criminals' hands. Lenders and credit report agencies themselves may with or without intent sell this information to criminals.

In addition, there are many private agencies and government organisation, such as

---

[142] J G Ronderos 'Identity Fraud and Transnational Crime' A Paper Presented for Seven Meeting of the CSCAP Working Group on Transnational Crime Manila Philippines Galleria Suites May 31June 2000 available at <http://www.ncjrs.gov/nathanson/id_fraud.html> accessed on 26 May 2011

[143] A Steel, 'The True Identity of Australia Identity Theft Offences: A Measure Response or Unjustified Status Offences?' (2010), Vo. 33 (2) University of South Wales Law Journal 503-531; Adams 'The Identity Theft Project Report' and Assumption Deterrence Act of 1998: How Effective Is It in Combating Identity Theft' 15 December 2001, 1 available at <http://gsulaw.gsu.edu./lawand /papers/fa00/adams> accessed on 26 May 2011

[144] M CHawki and M Abdel Wahab, supra, note 67, 11

[145] L LoPucki, 'Did Privacy Cause Identity Theft?' (2002-2003) Vol. 54 (4) Hasting Law Journal 1277-1298

[146] ibid 1283

banks, video stores and Depart Motor Vehicle centres collect the individuals' information. Those agencies may facilitate the commission of identity theft if they fail to shred unneeded documents or use unsecure computers that criminals can hack into them and steal the personal information that held in. They may also disclose with or without intent the personal information of costumers to criminals who may use it to commit other crimes.

Owing to the personal information of people in held many agencies; the individuals may find it is difficult to control their information. It may be easy for any other persons to obtain this information, and then uses to carry out illegal activities. Additionally, some financial institutions may sometimes not declare the great breaches of individuals' personal information that happened in their records[147] and that may facilitate identity theft occurrence.

It seems from the analysis of this chapter, that Iraqi legislation does not contain a definition of identity theft. In addition, academics in their literature and legislatures in other jurisdictions have defined in different ways. As a result, there is no a universal definition of identity theft. The difference and the lack of the definition of identity theft may lead to inaccurate determination of its elements.

2.7 Conclusion:

Under Iraqi legislation, unlawful acts that are committed against intangible materials have not been defined. Iraqi legislators do not determine whether taking intangible property as a crime. As a result, identity theft is a type of crime that is committed against intangible materials is not defined in Iraqi legislation.

To determine a precise definition of identity theft, the thesis in this chapter has attempted to analyse the definitions that have been stated by some scholars and legislations in other jurisdictions. Many scholars and countries, such as United States, Canada and Australia have attempted to define identity theft in their legislations as they so deemed. However, there is no single acceptable definition for identity theft.

In addition, the situation of the UK legislature regarding the definition of identity theft

[147] Canadian Internet Policy and Public Interest Clinic (CIPPIC), supra, note137

is unclear. The UK legislature does not define identity theft offence and does not consider it as a separate crime. It was noticed that the UK courts also do not define identity theft. They attempt to explore some rules that may relate to identity theft offences from different laws, such as the Fraud Act 2006. Consequently, one cannot exactly determine what these provisions mean. Moreover, the person does not know when he may be guilty of identity theft if he uses wrongfully another person's information.

Due to the lack of legal provisions that define identity theft as a crime in Iraq and the difference in the definitions that have been sat out by academics and legislatures in other jurisdictions, the study has remanded the Iraqi legislature should sufficiently define identity theft or it should at least mention the main traits of this crime. The study has presented a definition of identity theft, so the Iraqi legislature can adopt it.

Exploring the definition of identity theft in Iraqi laws, literature and some jurisdictions of other states has led to examine the features of identity theft, factors that may facilitate the commission of it and some other issues. Thus, the study showed that an identity theft offence has many features that make it an uncontrolled phenomenon. Occasionally, it can be committed via the internet remotely. Criminals may target any computers that held important governments and individuals' information irrespective of whether it is connected with the world network. Perpetrators also use sophisticated methods to commit identity thefts and they have the ability to conceal crimes evidence. As a result, they may commit their crimes without detection.

It was shown in this study that a main victim of identity theft is people, but identity theft effects may extend to encompass companies, banks, members of governments and lenders. Identity theft targets everyone in the world society irrespective of whether he is alive or dead, an adult or a child, an ordinary person or a person in high status. As a result of stealing personal information of another person, and then use it to commit other crimes, victims of identity theft offences may suffer many effects, such as financial and non-financial effects. In addition, they and their family may suffer side effects, such as harassment by other persons, such as lenders or they may suffer disintegration of the family.

The present study revealed that identity theft is a crime differs from other forms of

crime, such as identity fraud and identity crimes. It also showed that there are many factors may assist perpetrators to carry out identity theft and facilitate the commission of it, such as the relationship between victims and perpetrators, the victims' negligence and the internet. The internet is considered to be one of the main factors that contribute in identity theft diffusion. It shown in this study some scholars argued that the internet creates identity theft. However, this view may be incorrect because identity theft is a crime that has prevailed ever before the internet emergent. The internet may facilitate the commissioning of identity theft, but does not create it.

As the issue of the definition of identity theft offence under Iraqi laws, definitions of identity theft in academics' literature and other jurisdictions has been addressed, it is more important to examine in the next chapter the elements of identity theft in order to explore an accurate legal framework to fight identity theft.

Chapter Three

How Identity Theft Takes Place and the Distinctive Legal Elements

Introduction

Due to Iraq having no specific law to cover identity theft and given that both theft offence laws and the project of 2011 contain no a clear definition of identity theft in which one can determine the elements of identity theft, the thesis will attempt to examine the elements of identity theft in regarding to the perspective of literature and legislation in other jurisdictions. Determining these elements will assist in answering the question of whether Iraqi criminal courts can find or create a workable legal framework in current laws, such as the current theft offence laws, to govern identity theft.

Identity theft is not different in the concept from conventional theft. Both identity theft and non-identity theft offences consist of a subject of theft, which should be protected by the rules of the law, and conduct that causes breach of these rules of law. The conduct should be counterbalanced as well by the sanction of the State. However, the primary difference between theft and identity theft is that identity theft is a crime committed against an intangible thing (a person's means of identification), while traditional theft is committed against a tangible property. Identity theft can be committed by employing two types of methods, namely sophisticated methods and non-sophisticated methods. Some of these are not physical actions. In identity theft offences, the person may not be deprived of his means of identification when it has been taken by another person, whereas in theft offences the owner is deprived of his property. These points of distinction between identity theft offences and traditional theft offences (tangible and intangible, physical and non-physical and depriving the owner from his property) create new challenges that require legal analysis and legislation to be amended appropriately. These challenges will be discussed in the next chapter.

Generally, identity theft as in any other crimes that are committed against a person property consists of two main elements: *actus reus* and *mens rea* and a third element that is represented by an identity or a means of identification belonging to another person or what is referred to as the subject of theft. As stated in Chapter One, there is a

difference between the crime and its effects. Sometimes the crime, such as possession of a weapon or identity theft, is used to commit other crimes, but this does not mean that the former crime is committed when it is used 'as a means' to commit other crimes. It has been committed at an earlier stage. Possession of a weapon, for instance, is committed when the accused has bought the weapon to commit other crimes. Therefore, identity theft also is deemed to have been committed when the accused has obtained another person's means of identification without consent, with intent to commit other crimes and not when he later uses it to commit these crimes. Some jurisdictions (such as the US and Australia) criminalise the theft of a person's means of identification when this is used *to commit other crimes only*. Consequently, according to those jurisdictions, the *actus reus* of identity theft consists of the transferring of, the possession of, or the use of another person's means of identification to commit other crimes. Other jurisdictions (such as the UK) do not consider identity theft as a separate crime, and thus it is difficult to determine the elements of identity theft in these jurisdictions.

According to some scholars' perspectives, the *actus reus* consists of illegal and legal activity to commit identity theft. This activity refers to the appropriation or the methods that are used to commit identity theft. Identity thieves may use two types of methods to carry out their crime: (1) low technology methods (such as dumpster diving and shoulder spoofing) and (2) high technology methods, (such as phishing or spam). Some sophisticated methods stand alone as crimes and cause challenges for Iraqi legislation. They need to be criminalised within the context of a specific law.

To scrutinise whether these elements could be found in the current Iraqi laws, such as theft offence laws or the 2011 Project, the author will discuss in this chapter in two sections the traditional and the non-traditional, or so-called offline and online methods, that are used to commit IT crime. It is important to show how identity theft occurs and how identity thieves can obtain sensitive data[1] of victims to achieve their crimes. In order to give a fully comprehensive analysis of the *actus reus*, participation in identity theft as a part of it will be discussed. In addition, another person's means of

[1] P J Bonneau and J W Hajeski, 'Identity Theft- Is It a Cryptographic Problem?' an Interactive Qualifying Project Report Submitted to the Faculty of the Worcester Polytechnic Institute, Number 52-BS2-0402 March 14, 2005, 6 available at <http://www.crypto.wpi.edu/publictions/Documents/WPI_IOP_IdTheft.pdf> accessed on 27 September 2010

identification as a subject of theft and the element of belonging to another person's will be discussed. The *mens rea* will also be discussed in this chapter.[2]

3.1 *Actus Reus*

Generally, the *actus reus* of crimes committed against a person's property is an act or behaviour that has been conducted by a person to appropriate it. The *actus reus* of identity theft could be an illegal or a legal activity that may be committed by a person to obtain another person's means of identification, transferring, possessing, and using it to commit other crimes[3]

3.1.1 An Illegal or a Legal Activity

'An illegal or a legal activity' is an act in which a person can obtain a means of identification of another person. An illegal activity constitutes a main method that can be used to obtain another person's means of identification. As stated above, some jurisdictions state that the *actus reus* of identity theft consists of transferring, possession, and using another person's means of identification to commit other subsequent crimes. These elements will be discussed later in chapter six to analyse in detail whether or not they are genuine and corresponding to the *actus reus* of identity theft. In the present chapter, traditional and non-traditional methods that may be used by criminals to obtain a person's means of identification will be discussed.

3.1.2 Obtaining a Person's Means of Identification

Identity thieves can obtain a person's means of identification by using one of two types of methods: traditional and non-traditional methods. These two different types will be discussed in the following two sub-sections.

3.1.2.1 Traditional or Offline Methods

Traditional methods include simple or non-sophisticated methods, such as stealing an individual's wallet or purse, chequebook, credit card or searching in his or her waste

[2] By extrapolating scholarly literature and some legislation of other jurisdictions, the author observes that the *mens rea* of identity theft consists of knowingly obtaining another person's means of identification without their consent, and then using it to commit other crimes.

[3] Identity Theft and Assumption Deterrence Act 1998 (a) (7) Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998)

(dumpster diving). Criminals may use these straightforward and basic methods to obtain a person's means of identification. Such traditional methods of stealing are described more fully as follows:

3.1.2.1.1 Purse or Wallet Loss or Theft

Taking away or stealing an individual's wallet or purse is a commonplace act used to carry out theft, as a means of obtaining money. What has become new in this traditional approach is the obtaining of a person's means of identification in order to commit other crimes. Most people prefer keeping their personal documents, (credit cards, social security numbers, driving licenses, or any other sensitive information) in their wallets or purses, or else in a safe place because where they believe that these documents should be remained in unexpected situations. Thieves now steal people's wallets or purses to carry out crime of identity theft. By stealing wallets or purses, criminals usually now obtain a person's means of identification.[4]

Thieves may get hold of wallets or purses in many ways. They may for example, steal the wallets or purses from the owner's hand or from his/her pocket, car, clothes, or bags. For instance, a ring of criminals in 2006,[5] rented cars and drove to lots of outdoor recreation areas in order to steal tourists' wallets or purses left in their cars. In addition, after a criminal has found a lost wallet or purse, he may phone that person, and tell him that he has found the lost wallet or purse. He may then ask the owner of the wallet or purse for more personal details. If the owner reveals the information that is requested the criminal may use this to commit other crimes.[6] This method allows the criminal to commit identity theft more easily. Stealing an individual's wallet or purse to obtain personal information is the method that is mostly used to carry out identity theft, more often than computer misuse in fact, another method (as an alternative method) used to obtain someone's means of identification and to commit identity theft.[7]

---

[4] P J Bonneau and J W Hajeski, supra, note 1, 9; *United States of America v. Corey L. Hines*, United States Court of Appeals, 472 F. 3d 1038 (8th Cir. 2007); *U. S. v. Williams* 355 F.3d 893, (6th Cr. 2003) Fed. App. 0453P

[5] *United States of America v. Karen Battle*, United States Court of Appeals, No. 10-1984 (3rd Cir. 2011) unreported

[6] O Angelopoulou, P Thomas, K Xynos, and T Tryfanos, 'On-line ID Theft Techniques, Investigation and Response' 2007 Vol. 1 (1) Int. J. Electronic Security and Digital Forensics 76-88; B Dwan, 'Identity Theft' (2004) Vol. 2004 (4) Computer Fraud and Security 14-17

[7] P J Bonneau and J W Hajeski, supra, note 1, 9

Stealing individuals' identification from government computers is another method that may be used by identity thieves. Criminals can obtain personal information from the government itself by stealing hard drives of computers from offices. Government computer hard drives are likely to contain information concerning the background and personal details of all government employees.[8] In 2005, for example, a thief stole a laptop from an office in the University of California in Berkeley that contained the personal data on 100,000 graduates, graduate students and prospective applicants. The data stolen included names, social security numbers, and in some cases the dates of birth and addresses of the students.[9] The data was accessed from the laptop belonging to university (in spite of the computer having a security code). The information was unencrypted.[10]

Moreover, criminals can obtain an individual's information by conspiring with or bribing companies' employees, government officials or persons who work for service organisations, such as banks, hospitals, or schools.[11] Occasionally, the identity thief may himself work as an employee for a company or government department. He may pretend as an employer, to be looking for other employees in order to access individuals' information and to steal it. Schreft[12] reported details a case in August 2007, in which, the two methods mentioned above were combined to carry out identity theft. In this particular case, criminals applied and registered as potential employers with Monster.com, the job-research website, seeking out new employees, in order to reach biographical information sites and to steal users' information, such as names, addresses and other sensitive information. They stole the information on 1.6 million users and

[8] K Zaidi, 'Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada' (2007) Vol. 19 (2) Loyola Law Review 99-150; *Krottner v. Starbucks Corp*, United States Court of Appeals, ,628 F. 3d 1139 (9th Cir. 2010)

[9] Berkeley 'Theft Exposes Data of 100,000' AP Associated Press (28 March, 2005) available at <http://www.msnbc.msn.com/id/7320552/ns/technology_and_science-security/t/berkeley-theft-exposes-data/> accessed on 30 Oct. 2010

[10] Testimony, at <http://judiciary.senate.gov/testimony.cfm?id/=1437& i729> in S Sproule and N Archer, 'Defining Identity Theft – A Discussing Paper' McMaster eBusiness Research Centre McMaster University 2006 27 available at <http://www.business.mcmaster.ca/idtdefinition/IDT%20Discussion%20Paper%20Revision%20from%20Sue%20Sproule%20April%206%2006.pdf > accessed on 10 August 2011

[11] G R Newman, M M McNally, 'Identity Theft Literature Review' (2005) 43 available at <https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf> accessed on 10 August 2011; *United States of America v. Karen Clark*, United States Court of Appeals, No. 10-10801 (11th Cir. 2011) unreported

[12] S L Schreft, 'Risks of Identity Theft: Can the Market Protect the Payment System' (2007) Fourth Quarter Economic Review Federal Reserve Bank of Kansas 5-40

then[13] used this information in many phishing schemes.

3.1.2.1.2 Stealing Mailbox Contents

Mailboxes are considered rich sources of personal information, which can assist identity thieves to obtain people's means of identification easily. In particular, many mailboxes are more vulnerable to theft because they are not correctly locked or protected.[14] Moreover, in automated credit bureaus theft of mailbox contents is made easier because credit agencies do not confirm the address when it is changed, or even inform the consumers who is the main subject in the change process.[15] Consequently, any person can easily open the post-boxes and take its contents without the original owner of the post-box knowing. The mailbox frequently contains sensitive information, such as pre-approved credit cards, bills and bank statements or other information. Therefore, it has become a high-reward goal for identity thieves.[16] For this reason, mailboxes ought to be secured. If mailboxes are left unsecured, the perpetrator can look inside them, and access the contents in order to use them to carry out other crimes.

Identity thieves can use many ways to carry out mailbox theft, such as the traditional method of looking through the post-box and taking its contents[17] or using an illegal duplicate mailbox key.[18]

They may also use ingenious methods, such as using sticky implement to retrieve mail from mailboxes. This candle a heavy object wrapped with a burly glue matter, such as

---

[13] S L Schreft, supra, note 12, 15

[14] P J Bonneau and J W Hajeski, supra, note 1, 7; F Paget, 'Identity Theft' MacAfee Avert Labs, White Paper l, 2007, 6 available at <http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf> accessed on 15 November 2010

[15] A Cavoulcian, 'Identity Theft: Who's Using Your Name? Information and Privacy Commissioner/ Ontario' 1997, 4 available at <http://www.ontla.on.ca/library/repository/mon/10000/197561.pdf> accessed on 21 October 2010

[16] M T Biegelman, *Identity Theft Handbook: Detection, Preventing, and Security* (2007), 33

[17] G Gerard, W Hillison, and C Pacini, 'What Your Firm Know about Identity Theft' (2004) Vol. 15 (4) Journal of Corporate Account and Finance 3-11

[18] *United States of America v. Thomas Dale Peterson*, United States Court of Appeals, 353 F.3d 1045 (9th Cir. 2003), The recruitment of youngsters is another way that may be used to steal physical mailbox contents. The criminal may also recruit youngsters to gather information about individuals in the marketplace and to steal from them, by pickpocketing. This method was used in 1996 in Puerto Rico (U.S) when criminals employed juveniles and gave them instructions to gather discarded data from the marketplace and then send it to the criminals by mail. In fact, gathering the disregarded information and sending it to the criminals via mail was a way to conceal the main purpose that the juveniles were told by criminals to do. The main purpose was stealing government cheques that had been placed in the mailbox or any other personal information, which might assist them in later carrying out identity theft.

pine tar or melted mousetrap glue, and attached chain. One of the criminals keeps a look out, the other puts the device into a mailbox through its slot and then with letter now attached pulls up the device with some of the mailbox contents.[19] This technique was used in Los Angeles in 1996, when postal inspectors there found it was being used to steal the contents of their mailboxes.[20]

Instead of stealing mailbox contents, a perpetrator may deceptively complete a change-of-address form at the Post Office or at credit card providers to obtain someone else's post, or any documents that contain an individual's information and is then readdressed to the perpetrator's address or postal drop-off point.[21] In addition, the perpetrator(s) may conspire with a personnel employee, or bribe him to steal the post that contains individuals' private information, such as pre-approved credit card applications, or credit card statements[22] or any other number of documents.

However, identity thieves may not steal mailbox contents, such as fax numbers, or voice mailbox, the information can also be obtained accidentally. Criminals may then use individuals' identities found in these contents and use it to commit other crimes.[23] A mailbox is considered a main store for individuals' information, and perpetrators find it easier to obtain information by stealing its contents or changing an individual's address.[24] Criminals sometimes do not need to steal the contents of mailboxes; they may find these contents thrown in dumpster bins.

3.1.2.1.3 Dumpster Diving

'Dumpster diving' is a term used to describe the activities of criminals who rummage through a person's garbage bags to find documents within them containing personal information, such as bill payment records, pre-approved credit cards, passwords, or bank statements, and then use this to obtain individuals' means of identification.[25]

---

[19] M T Biegelman, supra, note 16, 33; S F H Allison, A M Schuck, and K M Lersch, 'Exploring the Crime of Identity Theft: Prevalence, Clearance Rats, and a Victim/ Offender Characteristics' (2005) Vol.33 (2005) Journal of Criminal Justice 19-29

[20] M T Biegelman, supra, note 16, 33

[21] *United States of America v. April Nicole Garret*, United States Court of Appeals, No. 08-4933 (4th Cir. 2011) unreported

[22] G R Newman, M M McNally, supra, note 11, 43

[23] ibid, 4

[24] A Cavoukian, supra, note 15, 4

[25] P J Boneau and J W Hajesi, supra, note 1, 8; G Gerard, W Hillison, and C Pacini, supra, note 17, 4

Private personal information, such as bank account numbers, social security numbers, and pre-approved credit cards, are continuously recorded in documents and shared between the issuers and the owner of the information. As a result, many parties may have control on this data, such as banks officials, credit agencies, and corporation workers. If those parties do not properly discard or shred these documents and instead throw it intact in the rubbish bins, identity thieves may find these documents, and then use the means of identification that may be found therein to commit other crimes.

Searching an individual's rubbish bin is not encroaching on confidential private property. Consequently, dumpster diving is considered a perfectly legitimate. This was confirmed in a decision taken by the Supreme Court of United States in the case of *California v Greenwood*.[26] The facts in this case were that in 1998, the police without a search warrant looked through the trash bin of a Mr. Greenwood; an infamous drug dealer, in order to obtain information to assist them in proving his illegal activities and financial ventures. The police found documents indicating criminal behaviour. The court decided that information in receptacles for rubbish might be taken by anyone; therefore, the police behaviour was not illegal. This decision gave immediately everyone a right to look through garbage receptacles found in public places to obtain whatever items.[27]

Unlike the USA court, under the UK Theft Act 1968 everything that belongs to another should be subject to theft regardless whether it is inside his house or outside it unless that person entirely abandons it.[28] Thus, the UK courts consider the properties in a waste bin belong to the owner until they have been taken away by the refuse collector, and taking them without consent constitutes theft.[29] In addition, if a person lacks the

[26] *California v Greenwood*, Supreme Court of United States, 486 U.S. 35 (1988)
[27] P J Bonneau and J W Hajeski, supra, note 1, 8; *United States of America, v. Gustavo Villanueva-Sotelo*, United States Court of Appeals 515 F. 3D 1234 (2008)
[28] BBC News, 'Who, What, Why: Is Taking Rubbish Illegal?' 31 May 2011, available at <http://www.bbc.co.uk/news/magazine-13037808> accessed on 12 May 2014
[29] *Williams v Phillips*, Division Court (1957) 41 Cr. App. R. 5; (1957) 121 J. P. 163; Under the UK Theft Act 1968 a person may be guilty of theft if he takes anything that is owned by another person. The UK legislature in section 1 of The Theft Act states that: "(a) person commits theft if he dishonestly appropriates property belonging to another with intention to permanently depriving the other of it" for example, on BBC news it was stated that a woman has been accused of theft when she took potato waffles, pies, and 100 packets of ham from a bin outside of a Tesco Express in Essex, BBC News, 'Who, What, Why: Is Taking Rubbish Illegal?' 31 May 2011, available at <http://www.bbc.co.uk/news/magazine-13037808> accessed on 12 May 2014

mens rea of theft he may not be guilty of theft.[30] Although gathering of personal information from rubbish bins is a despicable act, it is more widespread than most people think.[31]

3.1.2.1.4 Theft in the Workplace

Employees working in institutions (such as banks, companies, or government institutions) may also be considered a useful means by which criminals can obtain individuals' information. This issue will be discussed in this section.

An individual's means of identification are collected by Businesses or State Services for genuine reasons. However, this may be taken by identity thieves. They can use several methods (such as bribing employees, or applying for a job in the company and even pay money to obtain a job in the business) in order to access an individual's information and then steal it to commit other crimes.[32] Employees sometimes can obtain a person's information illegitimately, and then use it to carry out other crimes, or sell this information to a third person who may himself use it to commit other crimes.[33] For example, it is stated that an employee stole a work colleague's information, found in the employer's locker that was left unlocked. Subsequently, the employee attempted to blackmail his co-worker.[34]

Theft in the workplace can be illustrated by another case that was mentioned by Cole and Ring,[35] the case happened during 1990. In mid-1990 to August of 2000, the criminal was a help-desk employee at Teledata Communications, Inc., a Long Island Computer Software Company that provides banks with computerized admission database including credit data; he had stolen information, such as passwords and codes for downloading consumers' credit reports, and then sold them to an unknown

[30] BBC News, supra, note 28
[31] C A Morgan, 'Minimizing Identity Theft: Fact, Fiction, or Futile' 2007, 11 available at <http://faculty.ed.umuc.edu/~sdean/ProfPaps/Bowie/T3-0607/Morgan-C.pdf > accessed on 5-Oct. 2010
[32] P J Bonneau and J W Hajeski, supra, note 1, 9
[33] ibid, 9; *United States v. Todd A. Wills*, United States Court of Appeals, No. 06-6009 (10th Cir. 2007) unreported
[34] PRC, 'Cases from PRC Hotline, Privacy Rights Clearinghouse' (PRC 2004-2006) available at <http://www.privacyrights.org/cases/cases2004-2005.htm > accessed on 31 October 2010
[35] E Cole and S Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying and Theft*, (Elsevier / Syngress 2005)

conspirator.[36]

In regarding to obtaining people's means of identification from companies, banks, or government institutions in the above way, one should distinguish between the person who steals and the person who uses this means to commit other crimes or sells it to others. According to rules of participation, the person who obtains this means from these institutions is considered a principal factor in the identity theft offence, whereas the person who uses this means of identification is a secondary participant, if he commits the elements of the secondary participation in identity theft, such as aids, abets or induces that person to obtain another person's identity. However, if he does not commit the elements of participation in identity theft, he may not be guilty of participation in identity theft. He may be guilty of using stolen identity to commit other crimes. Violation of trust may be a subset of this type of theft and this can also be used to commit identity theft.

3.1.2.1.5 Theft by Violation of Trust

Some criminals can easily access trustful individuals' means of identification. [37] They may be friends, house cleaners, babysitters or roommates, or a person who is a relation, such as son, daughter, wife or husband; an employee; to name but a few potential victims. Those criminals can steal this means of identification without any difficulty because the victim may hold them in a high degree of trust.[38] For example, a female

---

[36] E Cole and S Ring, supra, note 35; Idtheft, 911.com: available at <http://www.identitytheft911.com/education/articles/art20040915guilty.htm> accessed on 31 October 2010; *United States of America v. Philip Cummings*1:03-cr-00109-gbd-1 (2004), on September 14, 2004, the criminal pled guilty of three account: (1) conspiracy to defraud the United States; (2) fraud by wire, and (3) fraud with documents. He was sentenced to 5 years in prison on account one, 14 years in prison on second account, 14 years on third account, and 3 years of supervised release. The prison terms are to be served concurrently with each other. In addition, he was sentenced to $ 15, 386,673 in restitution.

[37] *United States v. Marry L. Landrry*, United States Court of Appeals, No. 09-1877 (1st Cir. 2011) unreported

[38] C A Morgan, supra, note 31, 12; in *United States of America v. Mary L. Landry*, the perpetrator was employed as a customer account manager by MBNA, a credit card company, the perpetrator's job exactly related to collect the past due credit card account. She was granted a security clearance. Thus, she had easily access to customers' information, such as social security number and date birth. The MBNA Company terminated the perpetrator's job because she convicted with a drunk-driving crime. After that, she had employed in Verizon. She could access the customers' information, such as social security numbers and dates of birth. It opened an account with Verizon before she left her job with MBNA Company for cable, phone and DSL in her home. In addition, she tried to open new account in the customers' names in several banks, such as Chase bank and Discover bank. Her trying to open an account in customers' name succeeded with Chas bank but failed because she worried from internet security and

army employee in the United States army was a victim of identity theft undertaken by a relation who exploited the stopped military security. The criminal stole her identity and opened numerous accounts in her name. [39] He caused her great harm, distress and loss, such as losing her job. She also was not able to receive any financial help from government or credit bureaus. She was forced to leave the county and live in another county.

Absent-mind workers may also enable identity thieves to access and steal individuals' information. In addition, dishonest workers can access individual files, such as salary data, insurance documents, or bank data by deceit and steal the information to commit other crimes or to sell it to other persons with criminal intent.[40] For instance, in a case in the U.S, in 2003,[41] the director of a recruitment agency was able to access and steal the names, social security numbers, and the dates of birth of six individuals including soldiers and civilians who came to the recruitment agency to register. This criminal then used this information to gain credit cards via the internet. He transferred approximately $47,000 from his cards in this way.

So, methods used by identity thieves to obtain individuals' information are diverse and numerous. They can obtain people's information by observing closely PIN numbers are trapped in an ATM or when their personal details are revealed during overhead conversations.

3.1.2.1.6 Shoulder Surfing

Shoulder surfing is so called because the person committing the offence observes individuals from behind, or uses the zoom control on a camera, binoculars, or an iPhone to determine PIN numbers when these are being entered at ATMs. People

---

entered the 9s numbers. In addition, after she opened account with Chas bank couldn't prove her social security in the later her deal with Chas bank, *United States of America v. Mary L. Landry*, ibid

[39] A Cavoukain, supra, note 15, 7

[40] C A Morgan, supra, note 31, 12

[41] *United States v. Michael F. Kimble*, Sr., No.02-CR-549-A (E.D. Va.), July 17, 2003 (*U.S. v. Kimble*, 70 Fed. Appx. 113 (4th Cir. Va.) 2003); M J Elston and A S Stein, 'International Cooperation in Online Identity Theft Investigation: Hopeful Future but a Frustrating Present. Computer Crime and Intellectual Property' Section, United States Department of Justice P.O. Box 887, Frank Station Washington D.C. 20044-0887, 6-10, 2002 available at <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf> accessed on 10 August 2011

unsuspectingly may reveal such persons when on the phone,[42] or when giving their details information at financial institutions.[43] Public passengers are often the preferred targets for identity thieves[44] using shoulder surfing.

3.1.2.1.7 Social Engineering

The identity thief may pretend to be working for a legitimate body, such as a bank or company, in order to steal the personal or financial information. This is called social engineering. 'Social engineering' refers to an identity thief who is pretending to be a legitimate person or representative or legitimate organisations in order to swindle unsuspecting individuals into divulging information.[45] Social engineering requiring human interventions depends on accomplished social skills to induce victims into revealing information.[46] For instance, in a case that happened in Virginia USA, [47] the perpetrator pretended to be the third party vendor an intermediary contracted with the Virginia Department of Medical Assistant Services, to provide medical services - including medical transportation to medical patients in Virginia. Some of the medical services are provided by Virginia Premier, according to the Virginia Health Premier Plan, and other medical services are provided by a third party. Some information about patients is provided to the third party in this agreement. The perpetrator in this case obtained patient information, such as medical identification numbers, and then used this information in fraudulent activities to obtain got $308, 329, 00.

Criminals can use many methods in social engineering activities. For instance, they may pretend to be a clerk of a bank or some other legitimate company, and present themselves at another company or to an individual who typically has an account or a job with the bank or the company in question, asking them about some information, such account numbers, dates of birth, or any other such sensitive and private

[42] G Gerard, W Hillison, and C Pacini, supra, not 17, 4; A Cavoukian, supra, note 15, 4
[43] K Zaidi, supra, note 8, 99-150
[44] A Cavoukian, supra, note 15, 4
[45] P J Bonneau and J W Hajeski, supra, note 1, 10; N Aguero, B Gandy, R Laoang, J Mejia, B Vandlez, MIS 304 and F Fang, 'Cybercrimes and Countermeasures' 2010, 1-29 available at <http://public.csusm.edu/fangfang/Teaching/HTMmaterial/StudentProjectSpring2010/Group7Paper.pdf > accessed on 15 November 2010; T M Chen, M C Elder, and J Thompson, 'Handbook, Chapter 74, Electronic Attack' 2005, 12 available at <http://lyle.smu.edu/~tchen/papers/handbook2005.pdf> accessed on 14 November 2010
[46] T M Chen, M C Elder, and J Thompson, ibid, 12
[47] *United States v. Abdelshafi*, United States Court of Appeals, 592 F. 3d 602 (4th Cir. 2010)

information. When the criminal obtains this information, he may use it to commit other crimes or sell it to other persons with criminal intent. Boeaun and Hajeski,[48] for example, stated that in a recent case, which took place in America in 2005, a Choice-Point Company is a company located in Georgia. It held information on almost every consumer in America, and then subsequently, sold this information to employers; the proprietors or marketing companies and even to government agencies. To access the information held by the company, criminals pretended to be legitimate businesses and could steal information of American consumers.

In addition, in order to steal another person's identity, an imposter may contact a store, company or bank, claiming that there are problems with a targeted account holder and then ask the employee answers the phone about that person's personal information, and typically, the employee will reveal information because he or she cannot verify the caller.[49] The perpetrator may also use a phone to contact the victim in the pretending to be a bank clerk and ask about their information claiming there are some problems with his or her account. By this means, the criminal defrauds the victim into revealing his personal details, and then uses it to commit other crimes.[50]

Instead of using the phone to obtain means of identification, the perpetrator may use mail as a means of social engineering to defraud people into divulging information. For instance, criminals may send printed letters through the post claiming that a person has won a cash award or suggesting that they need to donate to a charity. Regardless of what the letters contain, use this method on a secondary means of obtaining an individual's personal details. A good example of this is the so-called 'Nigerian Scam.'[51] Even though criminals may use a variety of methods in social engineering, the goal is always the same, namely obtaining individuals' identifications that can be used to carry

[48] P J Boeaun and J W Hajeski, supra, note 1, 10

[49] *United States v. Bush,* United States Court of Appeals, 404 F. 3d 263 (4th Cir. 2005)

[50] G Gerard, W Hillison, and C Pacini, supra, note 17, 4

[51] The Federal Trade Commission of U.S explained the Nigerian Scam as [claiming to be Nigerian officials, businesspersons or the surviving spouses of former government honchos, con artists offer to transfer millions of dollars into your bank account in exchange for small fee. If you respond to the initial offer, you may receive "official looking" documents. Typically, you are then asked to provide blank letterhead and your bank account numbers, as well as some money to cover transaction and transfer costs and attorney's fees. You may even be encouraged to travel to Nigeria or a border country to complete the transaction. Fraudsters sometimes produce trunks of dyed or stamped money to verify their claiming. Inevitably, though, emergencies arise requiring more of your money and delaying the 'transfer' of funds to your account. In the end, there are no profits for you to share, and the scam artist has vanished with your money. See P J Beaun and J W Hajeski, supra, note 1, 11

out further crimes.[52]

It may be said that some traditional methods might make the commission of identity theft easier, and therefore they should be regarded as aggravating circumstances that increase the punishment of identity theft. Due to Iraq having no specific law to deal with identity theft, the thesis suggests that the Iraqi legislature should take these methods into account when it intends to enact a new law to fight identity theft. However, traditional or non-sophisticated methods of obtaining a person's means of identification are not the only method employed; the emergence of the internet and using it for financial transactions almost universally enables perpetrators to devise new and *sophisticated* methods to obtain a person's ID. Scam is a method used by criminals to defraud people into divulging their personal information. There is no information about the scam as a method to steal a person's means of identification. The reason behind this lack may be related to that Iraq having no law to deal with identity theft, thus, people do not report their victimisation to police. In addition, there is no literature about this method to obtain the personal information. The author observes that methods used by criminals to obtain personal information are the same in each country of the world, particularly, methods relate to the internet.

3.1.2.2 Sophisticated Methods

The ubiquitous use of the internet for transactions makes personal information –unless secure- available everywhere. Nowadays, everyone whether by a legitimate means or not, can quite easily acquire someone's means of identification. On the other hand, perpetrators themselves can discover and employ quite sophisticated methods to obtain information about individuals. Most sophisticated methods used stand alone as crimes in themselves. In the following section, these sophisticated methods will be illustrated. A question that arises is, should the Iraqi legislature, like most other jurisdictions, consider these methods as crimes in themselves or will criminalising identity theft be adequate by itself to cover them? This question will be answered in chapter six, where the legislative solution to this is discussed comprehensively.

[52] P J Beaun and J W Haieski, supra, note 1, 11

3.1.2.2.1 Malware

'Malware' is an abbreviation and contraction of the term malicious software.[53] 'Malware' computer programs designed to infiltrate and damage computers without the users consent. It is the general term including all the different types of threats to an individual's computer safety such as viruses, Trojan Horse, phishing and other types. A perpetrator creates a malware program to modify or to damage other software found on an individual's computer without their knowledge and consent.[54] The perpetrator uses two types of closely related programs to install malware programs: the malware itself and 'rootkits' programs. Rootkits are programs that use system attaching or modification to hide files, processes, registry keys, and other objects in order to hide programs and behaviours. The relationship between the two programs is mutual. Rootkits cannot be installed on a computer without using the malware program. After rootkits have been installed on an individual's computers, they can hide further malware programs that are introduced. Rootkits were devised specifically for malicious purposes. However, currently, rootkits can actually be benevolent or even beneficial. Both types of rootkits nevertheless are regarded as a category of malware programs.[55]

Rootkits probably are considered a great danger because they replicate themselves and spread throughout an individual's computer system. Moreover, they enable the criminal to control the infected system completely and then disappear.[56] Some rootkits are used by other malicious programs or may be hired by criminals to ensure that their malicious programs are not detected. Rootkits, once infecting a computer, are difficult to remove, other than by completely wiping the hard drive and reinstalling software.[57] The perpetrator can use many types of malware programs to obtain someone's means of identification. Examples are viruses, Trojan Horse, phishing and other types. These types are discussed below.

---

[53] A Weiss, 'Spyware Be Gone!' (2005 Vol. 9 (1) Networker 19-25; D B Owen, 'The State of Malware' (without year) 10 available at <http://danielowen.com/files/The_Stae_of_Malware.pdf> accessed on 3 November 2010; L Steven and N Altholz, 'Rootkits for Dummies 'Chapter 1, Much Ado about Malware' 2007, 10 available at <http://www.sec88.com/book/Sec/RootKits_FD.pdf> accessed on 10 October 2010

[54] *United States v. Gonzalez*, United States District Court, District of New Jersey, No. 09-10382-DPW (2009) unreported

[55] L Steven and N Altholz, supra, note 53, 10

[56] A Conry-Murry, 'Who Knows What Evil Lurks?' (2006) Vol. 21 (3) IT Architect 11-26; J Fontana, 'Rootkits Aren't Doom But Keep up Defences' (2006) Vol. 23 (16) Network World 20; D B Owen, supra, note 53, 10

[57] J Fontana, ibid, 20, F Hayes, 'Routed by Rootkits' (2006) Vol. 40 (16) Computer World 58

3.1.2.2.2 Viruses

The word "virus" 'is often used as a common term for all malicious programs, but technically a virus is a program or code that attaches itself to a legitimate, or an executable piece of software, and then reproduces itself when that program is run'. Viruses are small programs that get into other practicable programs.[58] They are pieces of code that are designed to copy once they have attached themselves to a host program.[59] They can be copied by modifying either a normal or an infected program.[60] They can spread and make copies of themselves to slot into each manuscript or any file that can be used to perform a program when it is opened. This feature is the distinction between viruses and other types of malware.[61] Viruses can spread via the web, floppy disks, USB drives, or any kind of device that is used to store electronic information.[62] Viruses copy themselves irrespective of whether there is vulnerability in the system of the computer or not. Consequently, they can spread to files that are used by other non-malicious software.[63] However, to be activated they do require the users to open infected programs, such as opening a contaminated program or a tainted file.[64]

Viruses once inside software can be transferred to other computers when the user shares files and programs with other users, such as the use sharing a computer, peer-to-peer, or by using tainted CDs, DVDs, or floppy disks.[65] The peer-to-peer means of transmission has become a great threat for companies, such as Sharman network Kazaa file sharing network. Due to these companies having a lot of users who use peer-to-peer file sharing, they have become a tempting goal for criminals.[66] When this file sharing is loaded on a computer, it enables every participant to access the computer and search in shared files.[67] Viruses may not be as harmful now as they were in the past. However,

[58] L Steven and N Altholz, supra, note 53, 11
[59] D B Owen, supra, note 53, 4
[60] T M Chen, et tale, supra, note 45, 14
[61] D B Owen, supra, note 53, 4
[62] N Aguero, et tale, supra, note 45, 17
[63] R Ford, 'Malware Briefing' (1998) Vol. 17 (2) Computer and Security 110-114 in D B Owen, supra, note 53, 5
[64] ibid, 110 in Owen, supra, note 53, 5
[65] ibid, 3
[66] G Lawton, 'Virus Wars: Fewer Attacks, New Threats' (2002) Vol. 35 (12) Computer Technology News IEEE Xplore 22-24
[67] S L Schreft, supra, note 11, 13

they can contain rootkits in their design,[68] which can be used to hide malware programs. Viruses can damage a computer's software that contains the running system by degrading information found on storage media and the writing found on file. [69] Moreover, they may be used to steal the users' information,[70] and then transmit it to the criminal who uses it to carry out further crimes.

3.1.2.2.3 Worms

Worms are programs that have the ability to copy themselves over a computer network. They often accomplish malevolent actions,[71] such as shutting down a computer, or using its resources.[72] They may take up residence in the random access memory (RAM) and can spread from one computer to others by emails, as a message program, or by peer-to-peer file sharing network.

There are many differences between worms and viruses. Viruses are program codes that are reproduced by modification of both an infected and a normal file, while worms are independent and autonomous and do not rely on other programs. Accordingly, worms are reproduced through propagation copies of themselves to other systems via the internet,[73] and do not have to integrate themselves in other programs. They depend on the vulnerability of the software system for spreading, instead of depending on an executing program that the user uses. Consequently, they usually spread without the user's interaction.[74] They rarely affect documents found on the hard drive of the computer. However, they can paralyze computers by making the information flow congested, slowing the operation of the system by using its sources, or by destroying the system entirely through creating numerous copies of themselves. Nonetheless, at

[68] L Steven and N Altholz, supra, note 53, 11
[69] ibid, 11
[70] K Spurlock and D Wyatt, 'The Internet Security Dilemma' 2007 California State University 12 available at <http://public.csusm.edu/fangfang/Teaching/HTMmaterial/StudentprojectSlides-Sprg2007/FinalPaper-1-5.pdf> accessed on 15 October 2010
[71] M Bhasin, 'Mitegating Cyber Threats to Banking Industry, Information Technology' 2007, 1618-1624 available at <http://www.icai.org/resource_file/96551618-1624.pdf> accessed on 27-Oct-2010; K Spurlock and D Wyatt, ibid, 4
[72] Bhasin, ibid, 1620
[73] T M Chen, et tale, supra, note 44, 14
[74] D R Ford, supra, 63 in B Owen, supra, note 53, 5; T M Chen, et tale, supra, note 45, 14; N Aguero, et tale, supra, note 45, 17

first, they need a long time to infect a system;[75] but when introduced can spread tremendously quickly to infect the entire system. For instance, one spreading of worms is estimated to affect 10,000 systems.

Worms can target unprotected computers that have no reform programs to fill security gaps. They can damage many computers in a network. They can shut down great portions of the internet before they are detected and stopped.[76] Moreover, they can carry with them other malicious programs, such as rootkits, backdoors, and Trojan Horse that are very important to the perpetrators seeking to steal an individual's information.[77] The 'bugbear' family is a good instance of a worm that has many malicious actions, which can both adversely affect computer systems and accomplish purposes for which perpetrators intended them.[78]

Criminals use various methods to send worms to invade individuals' computers. They may send emails that contain infected attachments to the target computers. The infected attachments that are sent by worms may need executing programs to infect victims' computers, or they may infect victim's computers by merely previewing or reading it. In addition, they may use peer-to-peer file sharing, the password guessing, or combine with one or more other malicious programs to ensure their successful propagating throughout a network.[79] After being successfully installed on victims' computers, worms begin to copy themselves and transfer to the target computers via emails or any assistant vectors, such as 'backdoor'.

3.1.2.2.4 Trojan Horse

Every user should be aware when using the internet, especially if he/she downloads a program or visits an unknown website, that often viruses or unsolicited material can be found on many websites, Trojan Horse is one of these viruses. It is a type of a spyware program that is installed surreptitiously on individuals' computers.[80] (The name of Trojan Horse is a reference to the clever invention of Odysseus –Ulysses- in the Greek

[75] P A Henry, 'Firewall Considerations for the IT Manager' (2005) Vol.14 (5) Information System Security 29 in D B Owen, supra, note 53, 5
[76] L Steven, and N Altholz, supra, note 53, 11
[77] ibid11
[78] M Bhasin, supra, note 71, 1621
[79] T M Chen, et tale, supra, note 45, 15
[80] L Steven and N Altholz, supra, note 53, 11

legends given as a cunning gift to the unsuspecting Trojans, dunning the siege of Troy). Trojan Horse can carry malevolent applications or devastating programs disguised as a useful program.[81] It is difficult to detect Trojan Horse cunningly because it hides itself with another benign program, and only appears when the user opens the benign program, typically to cause damage to his computer.[82] Sometimes, however, instead of damaging and even destroying an individual's computer, the Trojan Horse may instead steal the user's means of identification, such as passwords, credit card details, or any sensitive personal information.

The Trojan Horse is in expressions of technology specialists of information, which can be considered a helpful, or an interesting program that includes malicious cryptogram devised to damage a victim's computer.[83] In particular, some Trojan Horse programs are designed to disappear into the running system of the computer and spy on each key stroke. They exploit the vulnerability found in some computers to obtain individuals' information.[84] For instance, the perpetrator can spy on contaminated computers and gain the information that he needs to commit other crimes.[85]

The Trojan Horse can be managed remotely. It is used to deceive users to install and execute the program that contains Trojan Horse.[86] It exploits the system's vulnerability to install itself.[87] Trojan Horse once installed can perform whatever function that the criminal designed it to achieve, such as monitoring users' activities, downloading a file, presentation of the desktop in real time or recovering temporarily the stored

[81] L Steven and N Altholz, ibid, 11; M Chawki and M S Abdel Wahab, 'Identity Theft in Cyberspace: Issues and Solutions' (2006) Vol.11 (1) Lex Elicotronica 1-41;N Aguero, et tale, supra, note 45, 17
[82] N Aguero, et al, supra, note 45, 17
[83] P J Beaun and J W Hajeki, supra, note 1, 12; Y Lee and K A Kozar, 'Investigating Factors Affecting the Adoption of Anti-spyware System' (2005) Vol.48 (8) Communications of the ACM 72-77
[84] P J Beaun and J W Hajeki, supra, note 1, 12
[85] ibid, 12
[86] T M Chen, et al, supra, note 45, 13
[87] J C Sipior, T Ward, and R Rosell, 'The Ethical and Legal Concerns of Spyware' (2005) Vol.22 (2) Information Systems Management 39 in D B Owen, supra, note 53, 6; J C Sipior, T Ward and R Rosell, 'A United States Perspective on the Ethical and Legal Issues of Spyware' (2005) 738-743 available at <http://delivery.acm.org/10.1145/1090000/1089684/p738-sipior.pdf?ip=147.143.87.3&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1250596B31D2B4A344D3BE28130794FDD&CFID=340113954&CFTOKEN=87244268&__acm__=1371311495_bda9fc1ea0fc67815758963e7d4c32fb > viewed on 30 March 2012; R Thomson, 'Why Spyware Poses Multiple Threats to Security' (2005) Vo.48 (8) Communications of the ACM 41-43

passwords,[88] and then transferring this information to the criminal.[89]

A distinctive feature of Trojan Horse is that it has -besides the common spyware features- a feature that allows an outsider user to control the system by remote administration. It does not replicate itself when it is installed on the computer and not transfer earlier between computers. In these features make Trojan Horse distinct from worms and viruses.[90] In some instances, the thief can completely take control of another person's computer or even penetrate into the database of a company where individuals' identification is stored.[91] Trojan Horse can enter into computers in many ways. It can combine with email attachments that may be opened without scanning for viruses or it can be found in a website that the individual links with, before sending a website browser to prevent the scripts.[92] Regardless of the way that Trojan Horse may access an individual's computer; the purpose is the same; to steal the individual's information[93] whether directly from the keyboard operation or indirectly via a number of different platforms. This number of platforms transfers over the network and is installed without the individuals' knowledge or consent.[94]

3.1.2.2.5 Dialers

A dialer is a piece of parasitic software that can be used to cause the modem to call costly levy services, such as 1-900 numbers, international calls, and expensive 10-10xxx access codes.[95] Most dialers attach the phone numbers without the users' consent and submit phone charges to their bills.[96] It is used to make damaging, fraudulent and

---

[88] M Chawki and M S Abdel Wahab, supra, note 81, 20; Federal Trade Commission, 'Take Charge Fighting Back against Identity Theft' (Report) (2004) available at <http://www.talgov.com/tpd/pdf/tc-fbaidt0605.pdf > accessed on 20 December 2011

[89] T F Stafford and A Urbaczewski, 'Spyware: the Ghost in the Machine' (2004) Vol. 14 (2004) Communications of the Association for Information Systems 291-306

[90] M Chawki and M S Abdel Wahab, supra, note 81, 20; D B Owen, supra, note 53, 6; R Ford supra, 63 in Owen, supra, note 53, P A Henry, supra, 29 in Owen supra, note 53; Weiss, supra, note 53, 18; J C Sipior, T Ward, R Rosell, supra, note 87, 39

[91] ibid, 12

[92] L Steven and N Altholz, supra, note 53, 12, M Chawki and M S Abdel Wahab, supra, note 81, 20

[93] L Steven and N Altholz, ibid, 12

[94] D B Garie and R Wong, 'Parasiteware: Unlocking Personal Privacy' (2006) Vol. 3 (3) Scripted 203-220 available at <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-3/parasiteware.asp> accessed on 20 December 2011

[95] D B Owen, supra, note 53, 7; T F Stafford and A Ubaczewski, supra, note 89, 294; Weiss, supra, note 53, 18

[96] M Salhuana and L Groves, 'Investigation of Security Breaches of Popular Web Browsers' (2005) 15 available at <http://enpub.fulton.asu.edu/iacdev/courses/CSE494-

alleged calls.[97] There are two types of dialer programs found on web sites: benign and malicious.[98] A benign program is a program installed as a part of an operation system to help individuals connect with the internet via analog dial-up correlation. A malicious program is a program used to establish fraudulent correlation or to force certain files to download. Trojan Horse, *ActiveX and JavaScript scripts* can introduce a malicious program. In addition, a malicious program can be installed when an attachment is associated with a spam email.[99] Frequently, dialer is associated with pornographic websites.

Dialer affects the modem and causes damage to individuals' computers. As a consequence, it has no effect on individuals' computers that have no modems. However, it is still a malicious program in spite of it having no direct effect on individual computers.[100]

3.1.2.2.6 Backdoors

Backdoors are programs or alterations to existing programs that furnish external users with remote access to an individual computer without needing to identify their presence.[101] They pose themselves as benign programs or as a specific password in order to remain unseen. *Backdoors* attack either unpatched or unprotected computers. They can also attack the computer system directly by the *blackhat* hacker or by Trojan Horses, viruses, or worms. Moreover, genuine programmers of software can install as *Easter Eggs*.[102]

Easter Eggs are unseen programs found inside software that can execute special instructions. Professional programmers place *Easter Eggs* programs within commercial software, and then notify other programs of the way to access them to display, for example humorous animations or messages. However, sometimes they are employed as malware as easily.[103] Criminals can attack individual computers and steal information

598IA/Fall2005/files/projects/Final_report/Group1.pdf> accessed on 20 November 2010; K Spurlock and D Wyatt, supra, note 69

[97] A Weiss, supra, note 53, 20

[98] L Steven and N Altholz, supra, note 53, 12

[99] L Steven and N Altholz, supra, note 53, 12

[100] D B Owen, supra, note 53, 7

[101] L Steven and N Altholz, supra, note 53, 12, T M Chen, M T Elder, and J Thompson, supra, note 45, 13

[102] L Steven and N Altholz, ibid, 13

[103] ibid, 13

via *Bluetooth* that contains Backdoors programs that have established a trusted relationship during the use of a pairing machine in order to ensure their disappearance. This allows criminals to access an individual's information found on their electronic devices. Moreover, they can access the modem and the internet without the individuals' consent.[104]

Some *Backdoors* are used to promote legitimate activities, such as Sub 7, Back Orifice 2000, and Virtual Network Computer.[105] They are avoiding frequent access and evading security control, such as the login with password.[106] They can install key loggers and seize victims' information, such as credit card numbers or addresses of emails.[107] When Backdoors are installed on individuals' computer systems they leave it open for criminals.[108]

Backdoors allow hackers to remotely access victims' computers and obtain information.[109] Criminals accessing computers remotely by means of Backdoors programs illustrates why others programs, which resemble Backdoors in this function are named Backdoors.[110] Backdoors can become a host program and carry other malicious programs, such as worms. For example, the 'Doomjuice' worm can spread to other computers by using the Backdoor program that may be opened by 'MyDoom'.[111] According to a report carried out by the Trend Micro Company in April 2004, Backdoor programs represent 60% of malware programs that have been discovered.[112] They can be installed on computers by other programs, such as worms, spyware,[113] or Trojan Horse, which use Backdoors to display the user's information and the private

[104] P Suri and S Rani, 'Security Manager- Key to Restrict the Attack in Bluetooth' (2007) Vol. 3 (7) Journal of Computer Science 546-548
[105] T M Chen, M C Elder, and J Thompson, supra, note 45, 13
[106] ibid, 13
[107] L McLaughlin, 'Bot Spyware Spread, Causes New Worries' (2004) Vol. 5 (6) IEEE Distributed Systems Online, IEEE Computer Society 1- 5
[108] S Shetty, 'Introduction to Spyware Key Loggers' 04-4- 2005, 1 available at <http://www.securityfocus.com/print/infocus/1829 > accessed on 10 November 2010
[109] F Paget, supra, note 14; L Edwards, 'Down of the Death of Distributed Denial of Service: How to Kill Zombies' (2006) Vol. 24 (23) Cardozo Arts and Entertainment 23-62
[110] ibid
[111] ibid
[112] L McLaughlin, supra, note 107, 5
[113] L Edwards, supra, note 109

files.[114] The criminal then uses it to carry out other crimes.

3.1.2.2.7 Spyware

Currently, spyware is considered the greatest menace to internet and computer safety. It is defined as any software that gathers, sabotages, and reports information about internet users without their knowledge or previous approval.[115] This information includes every keystroke, the web browse practice email messages, credit card details or any other sensitive information. It consists of many applications that can hide themselves or inveigle the users in any way to thereby install themselves on their computers.[116] Spyware includes most types of malicious programs (except viruses and worms).[117] Spyware can control all or a part of the operating system of the computer.[118] Spyware is a method to control, observe, or to get benefit from another person without their knowledge or consent. If the spyware is successfully installed it is difficult to remove because spyware inserts itself throughout the system and uses a variety of methods to displace and replace files that are already a part of the normal operation of the user's computer.[119] If the user, for instance, "tears" some files, the hidden files will appear and replace the files that have been torn. Spyware that is run remotely by criminals, through using a remote website, can be used to recover and hoard individuals' data,[120] and then convey this data to the criminals.[121]

Identity thieves may offer free services, such as films, music, or antivirus protection to the internet users; however, they actually install spyware to steal individuals' information, such as their passwords, date of births, and any sensitive information, and

---

[114] K Curran, P Brisline, and K McLaughlin, *Hacking and Evasdropping* 2008; L J Janczewski and A M Colarik, 'Cyber Warfare and Cyber Terrorism, Information Science Reference' (2008) 309 available at <http://www.sclindow.net/MM/CyberWarfareandCyberTerrorism.pdf > accessed on 10 November 2011

[115] A Weiss, supra, note 53, 20; X Zhang, 'What Do Consumers Know about Spyware?' (2005) Vo.48 (8) Communications of the ACM 44-48; N F Awad and K Fitzgerald, 'The Deceptive Behaviours that Offend US Most about Spyware' (2005) Vo.48 (8) Communications of the ACM 55-60; D B Owen supra, note 53, 7; M Bhasin, supra, note 71, 1621; T R Loibl, 'Identity Theft, Spyware and the Law' (2005) 119 available at <http://delivery.acm.org/10.1145/1110000/1107650/p118-loibl.pdf?ip=147.143.87.91&acc=ACTIVE%20SERVICE&CFID=148923319&CFTOKEN=79497178&acm=1346339886_2a99b6c546d80e4fa40f98e3b7ac4341> accessed on 4 November 2010

[116] L Steven and N Altholz, supra, note 53, 13

[117] D B Owen, supra, note 53, 7

[118] L Steven and N Altholz, supra, note 53, 13

[119] D B Garrie and R Wong, supra, note 94, 206

[120] O Angelopoulou, P Thomas, K Xynos and T Tryfonas, supra, note 6, 77

[121] M Bhasin supra, note 71, 1621

then use it to commit other crimes.[122] Moreover, spyware can change the contents of the file, its name, or change the sites of installation every time that it is installed.[123] There are two types of spyware: (1) legal spyware and (2) illegal spyware. Both types of spyware can be used by malicious individuals to achieve control or to observe other persons' computers.

3.1.2.2.8 Ways That Are Used to Install Spyware

Spyware can be installed in different ways such as:

Spyware or adware may pretend to be from benign programs, but they are not. For instance, it may pretend to be an assistance program to help individuals to reach the web that they need easily or may help increase download speed. However, instead, it installs a malicious spyware program that is used to monitor individuals' activities on the internet and then conveys it to criminals.[124] In addition, it may pretend to be a program that removes the spyware threat, which may be found on a computer, but it presents a real spyware. Moreover, it makes users believe that their entrance is required, through mixing spyware programs with other programs that users need. As well, spyware programs may be provided with a peer-to-peer (P2P) file sharing.[125] Perpetrators use spyware or adware programs to obtain individuals' information, and then use it directly to carry out other crimes, or sell it to other persons who may use it to commit other crimes.[126]

The spyware uses the computer memory resources or bandwidths as a means to send the information back to spyware's home base when the user uses the internet. Using the memory as resources in running background may cause damage to the system, or to the common system instability.[127] A spyware program has the ability to observe keystrokes, or scan files on the hard drive, spy on other implementations, such as chat programs, or word processors. In addition, it has the ability to install other malicious programs, or alter the homepage on the Web browser. What is more, it can consistently transmit the individuals' information that has been obtained to the criminal who could use it to carry

[122] M T Biegelman, supra, note 16, 30; D B Garie, and R Wong, supra, note 94, 206
[123] D B Owen supra, note 53, 7
[124] M Bhasin, supra, note 71, 1621
[125] L Steven and N Altholz, supra, note 53, 14, 15, D B Garie, and R Wong, supra, note 94, 207
[126] L Steven and N Altholz, ibid, 17
[127] M Bhasin, supra, note 71, 1621

out other crimes, or sell it to another person.[128] Spyware programs use different channels (such as e-mail, file transfer protocol, upload to the net, or use chat room) to transfer the information that they have obtained to criminals.[129] It may also make a false rise in the number of the visits that are received by web in order to raise the income of advertising.[130]

3.1.2.2.9 Adware Programs

Adware programs are cookies that store individuals' information when users share with other internet websites,[131] or observe and shape the users' activities on the web[132] in order to obtain their information that may be used to carry out other crimes. Adware programs are, as the other malicious programs, installed without the users' consent.[133] These programs resemble spyware programs because they have similarity function. They can be used to observe the individual browsing to provide him or her with special advertisements, but they are not doing the same thing.[134]

However, adware programs differ from spyware programs where they are installed on individuals' computers with their approval, whereas spyware programs are installed on individuals' computers without their approval.[135] In addition, adware programs contain both benign and malicious programs. Furthermore, it is almost used for legitimate activities, to observe the user's activities, while spyware programs observe all the user's activities and everything that the user does with his/her machine. They also used to transmit the user's information to outside the entity.[136]

Although companies that provide programs in their computers frequently indicate that their programs are benign, they can clandestinely install adware programs. In fact, the proportion of the companies programs are benign, are fewer. They may be one in six.[137] Lawful adware programs vary from the unlawful adware programs; lawful adware

[128] M Bhasin, supra, note 71, 1621
[129] T M Chen, et tale, supra, note 45, 14
[130] K Spurlock and D Wyatt, supra, note 70, 5
[131] T R Loibl, supra, note 115, 119
[132] T M Chen, M C Elder, and J Thompson, supra, note 45, 13
[133] ibid, 14; T R Loibl, supra, note 115, 119
[134] D B Owen, supra, note 53, 7; L Steven and N Altholz, note 53, 13
[135] T R Loible, supra, note 115, 119
[136] D B Garie, R Wong, supra, note 95, 207
[137] L Steven and N Altholz, supra, note 53, 13

programs contain advertisements to compensate their production and maintenance expenses, while unlawful adware programs attack individuals' computers through showy ads, such as pop-up ads. Unlawful malware programs remain close to the user until he/she turns off his or her computer.[138] They can masquerade themselves as useful toolbars or research helpers and they appear as if they can do anything, but in effect, they do nothing.[139] Moreover, unlawful adware programs cannot easily be removed from an individual's computer, while lawful adware programs can easily be removed.[140]

Adware programs can redirect the individual who browses the internet, change his/her research outcomes, or provide targeted pop-up ads.[141] The adware program is a unique program. It differs from other malicious programs because it has a function, which is as advertiser driven. In addition, it observes the individual who is browsing the web sites and reports his activities to a centre database or implements ads on the individual based on the web habits.[142] Adware programs obtain the users' information when it is conveyed back to the marketing institute.[143] Some adware programs may change the manner that the browsing is working in, or `change the default browser setting, such as the homepage that individuals use, or reorient the searches to a different search system.[144]

3.1.2.2.10 Phishing

As noted previously, social engineering is a method that is used by criminals to obtain an individual's information, and then use it to commit other crimes. The difference between phishing and social engineering is that social engineering is a method that is used as a traditional means to obtain an individual's information, while phishing is a method that is used to obtain individual's information via the internet. Social engineering can occur in many ways whereas phishing occurs as messages that are sent via internet to induce people into divulging their information. Phishing can be defined

[138] L Steven and N Altholz, supra, note 53, 13
[139] ibid, 13
[140] L Steven and N Altholz, supra, note 53,13
[141] *United States v. Wallace L. Lawrence*, United States Court of Appeals, Tenth Circuit, No. 10-6257 (D.C.No. 5:10-CR-00011-D-1) (W.D.Okla.) (2011) unreported
[142] D B Owen, supra, note 53, 8
[143] T M Chen, M C Elder, and J Thompson, supra, note 45, 14
[144] D B Owen, supra, note 53, 8; S Shukla and F F Nah, 'Web Browsing and Spyware Intrusion' (2005) Vol. 48 (8) Communications of the ACM 85-90; T F Stafford and A Urbaczewski, supra, note 89, 292

as a means by which the criminal can dupe individuals to disclose their information by sending fake messages resembling messages that may be sent by the legitimate entities. It is called 'phishing' because it looks like the real fishing.

Phishing is email messages that are sent by the criminals to the internet users. In these messages, criminals falsely claim that they have established a legitimate venture in an attempt to defraud users into revealing their confidential information, such as a credit card details or account numbers, passwords, or any sensitive information that may be used to carry out other crimes.[145] Criminals incessantly send off surges of emails knowing that somebody will ultimately take the lure.[146] They may describe themselves as a popular company, such as eBay, PayPal, URL, or banks and send off bogus email messages to different customers.[147]

In their comments on a case of identity theft, Chawki and Abdel Wahab[148] stated that the criminal in this case for instance, pretended to be the Federal Bureau of Investigation and set up a phony website page completely resembling the Federal Bureau of Investigation website in order to obtain individuals' information, such as social security numbers, date of births, or any sensitive information. Due to many people wish to receive information from government they may easily fall victim of phishing. As a result, a website page like this may contribute in increase their belief in its authenticity. Users who visited this web revealed the sensitive information that has been requested and their credit cards numbers. Moreover, they paid ten dollars as fees for the application that they filled it, but they did not receive anything. Conversely, they have had to spend much time, money, and effort to repair the damage wrecked their credit history.[149]

In another case, a criminal during the period from 2001-2003, used a phishing to swindle internet users. He sent bogus emails that were designed to resemble official American Online and PayPal messages, to Internet users. Innocent receivers clicked on

---

[145] M Chawki and M S Abel Wahab, supra, note 81, 15; S L Schreft, supra, note 12, 12; M Bhasing, supra, note 71 1619-1620, F Paget, supra, note 14, 7
[146] P J Bonneau and J W Hajeski, supra, note 1, 13
[147] ibid, 12; B Graham, 'The Evolution of Electronic Payments, School of Technology and Electrical Engineering' the University of Queensland, October 2003, 23 available at <http://innovexpo.itee.uq.edu.au/2003/exhibits/s334853/thesis.pdf > accessed on 3 October 2010
[148] M Chawki and M S Abel Wahab, supra, note 81, 15
[149] ibid 15

the link, on the body of the email messages, and entered their personal information to this website. Then, the criminal recovered the information and used it to create new credit card accounts. The criminal targeted 400 victims and got from this process $75,000.[150]

Criminals might also send bogus emails that resemble those used by the Microsoft Network: it is possible that bogus emails could be directed to computer users. In these emails, criminals told users that there were difficulties arising from the last update that the company had done. As a result of this update, some consumers' information and the back-up system became inactive.[151] To confer the legitimacy on their email they might offer a free phone number for the consumer who might wish to call the company. They might also set up a web link and require users to click on it. The emails that were sent by criminals informed individuals that they had to enter their private information. However, after the users entered their information, they might discover that they were a victim of phishing.[152]

Contents of the messages that may be sent by the criminal(s) are various. The perpetrator(s) for instance, may tell the customer that the validity of his or her account has expired and it needs to be renewed. In addition, he/she may send a message to customers telling them that there is a breach in the company's security. On the other hand, he or she may declare some benefits for special members.[153] In all these types of phishing, emails that are sent by the thief will direct the consumer to a bogus web page. In this bogus page, the consumer will be asked to provide his personal information. Once this information entered into this page, it will be sent to the identity thief.[154]

Phishing is a phenomenon, not always sophisticated, but it exploits the vulnerability of the internet.[155] Internet-based payments, for instance, are attractive and more prevalent. They have fewer technology-oriented and marketplaces: therefore, criminals may exploit this disadvantage in the internet-based payments to send large emails to

[150] *Federal Trade Commission v Zachary Keith Hill*, United States District Court Southern District of Texas N. H 03-5537 (2004) unreported
[151] M Chawki and M S Abdel Wahab, supra note 81, 16
[152] ibid,16
[153] P J Beaun and J W Hajeki, supra, note 1, 12
[154] ibid, 12
[155] B Graham, supra, note 147, 23

customers ask them to update all their personal information. If the customers respond to these emails and reveal their means of identification criminals take it, and then use to carry out other crimes.

Graham[156] comments on a case as an example of phishing as a means to steal another person's identification. In this case, a criminal pretended to be PayPal Inc. and sent an email resembling PayPal's email to her client. The criminal in his email told the client that her account with the payment service provider was under examination because it became inactive. He requested her to confirm her new email address. The email included questions about her password, credit card details, and PIN number of her an ATM card. However, the criminal could not steal the client's information because the alarm bells rang and she phoned the company to tell it her worries about the illegality of this email.

Morgan[157] stated another example that may demonstrate phishing as a means to trick people into then revealing their means of identification. In this case, the criminal pretended to be the 'Internal Revenue Service' and sent a form of service attached within an email. The email included data and fax number. The criminal in his email warned the recipients and stated that if they did not fill the form and rapidly return it they might lose their tax exemptions.

Criminals sometimes use the phishing as a vocation and they do not want to obtain a benefit or cause detriment to another person. For instance, in 2004, the UK National Hi-tech Crime Unite arrested a 21 years old British man who was unemployed. The accused attacked a Co-operative bank, especially Smile Internet Bank. The team of Hi-tech Crime Unite reported that the accused was an amateur and did not associate with network criminal rings.[158]

According to the similarity between the email that may be sent by the phisher and the email that is sent by a legitimate entity, such as a company or bank, most individuals may fall victim to the phishing scams. For example, according to a research that has been conducted by the Association for Payment Clearing Services in the United

[156]B Graham, supra, note 147, 24
[157] C A Morgan, supra, note 31, 13
[158] S Hilley, 'Police Catch UK Phisher' (2004) Vol. (2004) (5) Computer Fraud & Security 1-2; O Angelopoulou, P Thomas, K Xyson, and T Tryfonas, supra, note 6, 2

Kingdom, four percent of online banking consumers fall victim to a phishing scam.

Phishing may be used to install some malicious programs (such as Trojan Horses, and key-loggers). In addition, it is used to install other programs like those without the user interference. It may remain inactive for a long period and wait until the user clicks, and then it traps him.[159]

3.1.2.2.11 Spoofing

Some scholars[160] believe that the spoofing program is considered to be a sophisticated type of phishing. However, other scholars[161] have refused to consider spoofing as a type of phishing. They believe that it is a different means in which criminals can hack into individuals' computers and steal their personal information. In fact, it could be argued that spoofing differs from phishing. Spoofing is a means that is used to dupe the individual(s) into revealing his/her private information through interception messages that are sent to them, and then changing their contents in order to make the individual believe that these messages are legitimate and are sent by their account. In addition, they may make entire changes to the message and resend it to other persons. While phishing is a means that is used to obtain individuals' information through setting up a bogus web resembling the legitimate web and then send a phony email to defraud individuals to reveal their personal information. However, spoofing is interconnecting closely with phishing and occasionally it is confused with it.

Spoofing can be defined as changing or counterfeiting an email address, or making an email that comes from different sources of addresses resembles the email that has been sent by the original web in order to make the internet users believe that it is issued from a genuine or trusted website. As a result of changing or counterfeiting the contents of the email by criminals, internet users may divulge their personal information (such as

---

[159] I Heller, 'How the Internet Has Expanded the Threat of the Financial Identity Theft, What Congress Can Do to Fix the Problem' (2007) Vol. 17 (1) Kansan Journal of Law and Public Policy 83-107

[160] K Zaidi, supra, note 8, 102

[161] M Chawki and M S Abdel Wahab, supra, note 81, 16, O Angelopoulou, P Thomas, K Xynos and T Tryfonas, supra, note 6, 78; W J Wang, Y Yuan, and N Archer, 'Identity Theft: A Contextual Framework for Combating Identity Theft' 2006, 30-38 Security and Privacy IEEE available at <http://see.xidian.edu.cn/hujianwei/papers/014-A%20Contextual%20Framework%20for%20Combating%20Identity%20Theft.pdf > accessed at 28-Oct-2010

their passwords, PIN, or social security numbers).[162]

In spoofing, criminals may attack the unsuspecting victims' website addresses and forge the contents of the messages that are directed to them to appear as though they are sent from their bank accounts, instead they may steal the victims' addresses that are found in the header page, and then use them to make emulation between their computers and the victims' computers. Therefore, they receive the messages that are sent to victims and then they steal their private information, such as passwords, credit card numbers, and other sensitive information.[163] Some scholars[164] mentioned that identity thieves might make a phony web page and send emails or advertisements resembling the legitimate businesses emails or advertisements that make consumers believe that they have come from their financial institution. Hence, they reveal their sensitive information, such as their names, addresses, credit card details, insurance plan digital, or social security numbers.

Furthermore, the criminal "spoofer" may send an email to individuals who have a bank account tells them that he/she is the manager of the system and requests them to change their passwords. Besides, he/she may threaten them with stopping their accounts if they do not respond.[165] In addition, the criminal may send an email pretending to be a person who has authority and asks them to send a photocopy of a password dossier or other sensitive information.[166] The spoofer may also pretend to be a service supplier, an identity theft prevention official, or personal internet service provider,[167] to defraud users into divulging their information to him/her.

In effect, criminals exploit the feature that a message when is sent to the owner it must pass through a number of users' computers during its transmission. Therefore, he/she can detect the personal information by using a sniffer to steal it. What is more, he/she may programme a device to select the information that is sent for any or every

[162] M Chawki and M S Abdel Wahab, supra, note 81, 16, I Heller, supra, note 159, 87
[163] M Chawki and M S Abdel Wahab, ibid 17
[164] K Zaidi, supra, note 8, 102, O Angelopourlou, P Thomas, K Xynos and T Tryfonas, supra, note 6, 79; A Cavoukian, supra, note 15, 4
[165] M Chawki and M S Abdel Wahab supra, note 81, 17; R Farrow, 'Source Address Spoofing: Forged Address Aid Internet Attaches. Here's what to Do about Them' Network Magazine 2001 available at <http://technet.microsoft.com/en-us/library/cc723706.aspx> accessed on 23 November 2010
[166] M Chawki and M S Abdel Wahab, supra, note 81 , 17
[167] W J Wang, Y Yuan, and N Archer, supra, note 161, 31

computer.[168] Additionally, criminals may modify or forge a part of or the whole message. If they modify or change the whole message, they can send it to numerous users to swindle them. By receiving the false messages, users reveal their information to criminals who then use this information to commit other crimes.[169] To complete spoofing, the spoofer may automatically send a message back to the sender to convince him/her that their email has been delivered to a genuine recipient.[170]

3.1.2.2.12 Skimming

Skimming is a method, which is used by criminals to read or hide personal information of other persons encoded on the magnetic strip of an ATM or a credit card.[171] A criminal uses a device that is called a skimmer to skim individuals' information. The Skimmer-device is an apparatus that resembles a beeper or a cell phone.[172] This apparatus is used to gather personal information of other persons (such as their passwords, SSNs, addresses and any sensitive information) that may be sent to them by emails from legitimate entities (such as businesses, government, or banks) via internet, or to intercept the emails,[173] and then redirect them to the criminal. Typically, a skimmer device is installed inside the machine, such as an ATM. If the customer passes his credit card or any credit through the machine the skimmer device will hoard the information that is found on the magnetic ribbon on the back of a credit or an ATM card.[174] Afterwards, this information is downloaded onto a computer or even transported onto an empty card.[175] Thereafter, the criminals can sign the back of the card.[176]

Skimming considerably takes place in restaurants, retail stores, or service stations because in these sectors the consumer is parted from his/her credit card when the

[168] M Chawki and M S Abdel Wahab, supra, note 81, 17
[169] M Chawki and M S Abdel Wahab, supra, note 81, 17
[170] ibid 17
[171] S F H Allison, A M Schuck, and K M Lersch, 'supra, note 19
[172] P J Bonneau and J W Hajeki, supra, note 1, 13; B Graham, supra, note 147, 25
[173] A Cavoukian, supra, note 15, 4
[174] P J Bonneau and J W Hajeki, supra, note 1, 13; F Paget, supra, note 14, 6
[175] Federal Trade Commission (2000b), 'Identity Theft Victim Complaint Data: Figures and Trends on Identity Theft. Retrieved November 20, 2000' available at <http://www.ftc.gov/bcp/workshops/idtheft/chart-update.pdf> accessed on 15 November 2010; Stuart F H. Allison, A M Schuck, and K M Lersch, supra, note 19, 20
[176] B Graham, supra, note 147, 25; S Sproule and N Archer, supra, note 10, 29; G R Newman, M M McNally, supra, note 11

skimming of consumer's personal information happens.[177] Usually, an employee in the restaurant or the retail store may own a skimmer device and use it to obtain the customer's information. A thief may sometimes offer money to the employee at the restaurant or petrol station to encourage him to steal the consumer's information.[178]

Skimmers may use many styles to skim information from credit cards. Criminals for instance, can interrupt the information cables from department repositories and other mercantile premises competent of duplicating documents that contain individuals' identification, such as credit card and 'Eftpos' data. Subsequently, they transmitted this information overseas.[179] In addition, criminals can amend the machine that the credit card is used in, such as an ATM,[180] or design an apparatus resembles the part of the machine and then place it on the card slit. After the consumer inserts the credit card into the machine, the apparatus will read its information that is found on magnetic strip and stock up this information.[181]

In *United States v. Stepanain*[182] for example, four co-defendants agreed to steal individuals' information (such as debit card numbers, personal identification numbers, and credit card numbers) from consumers of a 24-hour Stop & Shop grocery in Rhode Island. To accomplish their crime, they surreptitiously replaced the credit and debit card payment terminal in the Stop & Shop Checkout aisles with amended terminals. The amended terminal was provided with devices that recorded, or 'skimmed' debit card numbers, PIN codes, and credit card numbers whenever the customers swiped their credit card to make purchases. Then, they retrieved the converted payment terminal and replaced it with the store's original terminal. Criminals possessed the private account information of all customers who had used the machine through the converted period. Co-defendants had used this information to make aunthorised transactions, including cash withdrawals from the automatic teller machine (ATM). They were able to obtain in

[177] B Graham, supra, note 147, P J Bonneau and J W Hajeki, supra, note 1, 13
[178] P J Bonneau and J W Hajeki, supra, note 1, 13
[179] B Graham, supra, note 147, 25
[180] G Gerard, W Hillison, and C Pacini, supra, note 17 , 4; F Paget, supra, note 14, 6
[181] K Zaidi, supra, note 8, 101, the terms 'hacking and hacker' are defined in many definitions such as a: A person who enjoys exploring the details of programmable system and how to stretch his ability, as opposed to many users who prefer to learn only the minimum necessary. B: A person who enjoys the intellectual challenge of overcoming or circumventing limitation. For more information see M Chawki and M S Abdel Wahab, supra, note 81, 14
[182] *United States v. Stepanain*, United States Court of Appeals, No. 08- 1053 (1st Cir. 2009) unreported

total $132,300.

Thieves may also use the zoom of cameras to register the number sequence. After that, criminals use the information that has been registered to produce any card that they need to drain individual's accounts.[183] Another style that can be used by criminals encompasses placing a plastic sleeve in the card slit of the ATM to trap the card: when a victim places the card in the slot of an ATM and enters the PIN and nothing occurs, the criminal comes as a helpful person and tells the victim to enter their PIN number again; again, nothing happen and the card remains trapped in the sleeve. Ultimately, the victim leaves the card in the machine and goes to seek help to get the card from the machine. After the victim leaves the card in the machine and goes to look for help, the criminal comes and takes the sleeve and the card out of the ATM as well as the cash withdrawn.[184]

3.1.2.2.13 Hacking

A hacking is a method that can be used by perpetrators to access individuals' information with or without cyber trespass. It also means an unlawful access to individuals, government, pecuniary institutes, employers, creditors, or credit bureaus' computer systems to appropriate the individuals' information,[185] such as their names, addresses, social security numbers, or any other sensitive information. Actually, the computer system is often penetrated, and the information is diverted straight away or by using a listening device. Occasionally, this device is called a sniffer or scanner.[186] In April 2005, for instance, hackers could access the DSW Shoe Warehouse's computer system and stole information of 1.4 million credit cards and debit card transactions of 180 stores in the U.S. They also stole the account numbers of 96,000 cheque transactions.[187]

Some of the perpetrators could access the company's computer server, particularly the server of the ISP and steal individuals' information despite the security and the

[183] B Graham, supra, note 147, 26; F Paget, supra, note 14, 6
[184] H Clayton, 'Hole-in-the-wallet Machine' 2003 Financial Times (London) 22 in B Graham, supra, note 147, 26
[185] C A Morgan, supra, note 31, 13
[186] ibid 13; F Paget, supra, note 14, 6
[187] M Chawki and M S Abel Wahab, supra, note 81, 14

password fences that are found.[188] In another example, perpetrators hacked into an ISP computer server and appropriated records of 10,000 consumers.[189] Additionally, a hacker hacked into LexisNexis and almost stole information (such as social security numbers and driver's licence numbers of 300,000 individuals).[190]

In addition, identity thieves can acquire individuals' information from government institutions by hacking into their computer systems, which contain the information about individuals and their employees.[191] For instance, in a case that is considered to be the largest identity theft in the U.S, a hacker who was considered to be the mastermind of this identity theft and the leader of the ring hacked into U.S retail chains including TJX Cos and Barnes & Noble Inc., and stole millions of credit card and debit card numbers. Then he used them in fraudulent transactions.[192]

The hacker may use the trick or send an innocuous program to access the individuals' information, and then obtain it.[193] For example, he may use a software application to enter a commercial website, or the individual's computer. Furthermore, he/she may use the mirror keystrokes to obtain a credit card account details.[194] The criminal sometimes may decrypt its code if that is necessary, and then steal it.[195]

---

[188] M Chawki and M S Abel Wahab, ibid, 14

[189] ibid 14

[190] Press Release, 'LixesNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access' April 12, 2005 available at: <www.lixesnexis.com./about/releases/0789.asp.> accessed on 12 August 2011

[191] K Zaidi, supra, note 8, 102

[192] *U.S. v. Albert Gonzalez*, U.S. District Court in Massachusetts, No. 08-10223 (2009) unreported

[193] In his article, Levinson stated that Iraq's most prolific hacker is known as the "Iraqi Diver," an unidentified resident of Wasit Province, south of Baghdad, who has hacked into nearly 1,500 websites since 2005, according to Zone-H.org, an independent website that tracks and verifies hacker activity worldwide.
To date, the Iraqi Diver has usually refrained from causing permanent damage to sites, defacing them instead by leaving behind messages insulting President Bush or calling on the United States to leave Iraq. The list of sites that the Iraqi Diver has broken into include some of Iraq's most sensitive ministries, such as the Ministries of Interior, Electricity and Communications, and a handful of Iraqi banks, according to Zone-H. C Levinson, 'Hackers Attack Iraq Vulnerable to Cybercrime' USA Today, 29 August 2008 available at <http://usatoday30.usatoday.com/tech/news/computersecurity/hacking/2008-08-28-iraqhackers_N.htm?csp=tech> accessed on 30 May 2013.

[194] S Hoar, 'Identity Theft: the Crime of the New Millennium' (2001) Vol.80 (4) Oregon Review 1423-1447; G J Gerard and W Hillison and C Pacini, 'Identity Theft: An Organization's Responsibilities' 2004, 6 available at <http://ruby.fgcu.edu/courses/cpacini/courses/common/idtheftjoffincrim.pdf> accessed on 31 Oct. 2010

[195] F Paget, supra, note 14, 6

3.1.2.2.14 Key-loggers

Key-loggers can be defined as malevolent programs that are installed on individuals' computer systems without their consent. They consist of many malicious programs (such as *Trojan family*, *PHP*, and *A311 formxy.txt*). Each program of these programs gathers certain key strokes. They remain dormant until the user connects to the internet and gives them an opportunity to work. For instance, when the user accesses any website (such as Amazon or eBay) the key-logger will exploit this opportunity to steal his/her information, such as credit card information,[196] password, username, and any other sensitive information and send it to a custom host, such as a machine that enters this information into additional log files.[197]

Various keystrokes can be used to gather individual's information (such as his name, password, or any other confidential information) from their computer and transmit it to the offender. The offender may use malware programs that are installed on a host machine to receive this information. The machine may automatically send the information that has been stolen to the criminals.[198] Key-loggers are also used to steal businesses secrets.[199] Schreft[200], for instance, stated that in 2007, criminals sent an email, which contained key-logger programs to Monster.com to steal customers' information. Key-loggers had been installed on recipients' computers. When customers' opened the email, the key-loggers recorded their information (such as a bank account, password, or any other sensitive information) from keystroke and transferred it to the criminals. The key-logger program also affected their computers.

Criminals may use the keystroke-recording apparatuses that are found in the back of the computer where the connection of a keyboard cable is found, to steal a person's means of identification.[201] Paget[202] mentioned that in a recent case, which happened in 2005, criminals targeted the London office of the Japanese bank Sumitomo for several

[196] I Heller, supra, note 159, 88, F Paget, ibid, 8
[197] F Paget, ibid, 8
[198] K Curran, P Breslin, and McLaughlin, supra, note 114, 309
[199] G Lawton, supra, note 66, 23; D B Owen, supra, note 53, 6; P A Henry, supra, 29 in D B Owen, supra, note 53; J C Sipior, B T Ward, G R Rosell, supra, note 87, 39; S Shukla and F Nah, supra, note 144, 85; R Thompson, supra, note 87, 85; A Weiss, supra, note 53, 18; Y Lee and K A Kozar, supra, note 83, 72;K Spurlock and D Wyatt, supra, note 70, 7
[200] S L Schreft, supra, note 12, 15
[201] N Aguero, B Gandy, R Laoang J Mejia, B Valdez, MIS 304, and Dr. F Fang, supra, note 45, 20
[202] F Paget, supra, note 14, 9

months. At the first glance, the police who discovered the crime believed that criminals used a Trojan Horse program to accomplish their attacks, but it appeared from the investigation that they used a tiny keystrokes-recording apparatus. They inserted the apparatus in the back of the computer where the keyboard cable is connected. The criminals had taken the apparatus once it finished its mission after a period of time.[203]

Key-loggers can be installed surreptitiously on individuals' computers. They can also be remotely installed by an email. After their installation, they will use the email or the file transfer protocol to send the keystrokes, screenshots, and internet sites visited to the criminals.[204]

Non-traditional or sophisticated methods relate to the internet; therefore, users sometimes cannot distinguish between legitimate programs or emails and illegitimate programs or emails. In addition, some of these programs are installed surreptitiously: consequently, users may not easily discover them.

To summaries the above section regarding both traditional and non-traditional methods, it can be said that the literature and court decisions relating to identity theft indicate that traditional methods were used more than non-traditional methods in regarding to the committing of identity theft crimes. The reason behind the increase of use traditional methods to commit identity theft crimes is still unknown. It might be argued that the reason behind the increase is due to perpetrators becoming entrusted by other persons, who can thus easily access information and steal it. Occasionally, there is an already established relationship between criminals and their victims. This relationship and trust give criminals easy access to the victims' information. Traditional methods are straightforward methods, and are frequently used to commit identity theft.

The previous discussion has analysed important methods that can be used by criminals to obtain a person's means of identification to commit other crimes described by scholars and courts in several different jurisdictions in the world. However, legislatures of neutral major States, which consider identity theft a crime, such as US, and Australia, do not refer to these acts in laws that deal with identity theft. Also as shown in the previous chapter, neither the current Iraq theft offence laws nor the Iraq 2011 Project

[203] C A Morgan,supra, note 31, 14
[204] S Shetty, supra, note 108, 3

contain a definition of identity theft. Therefore, there is no legislative reference to these acts, which describe the above types of methods as a prohibited means of obtaining another person's means of identification. In effect, the social structure and the religion in Iraq may make the use of traditional methods to commit identity theft less often used than the use of sophisticated methods. Iraqi people may be more likely to be attacked by criminals who use sophisticated methods (such as phishing, hacking, spam or any other malicious programs) to commit identity theft from outside the Iraq rather than from inside it. It could be argued that traditional methods, which may be used by criminals to obtain persons' identities or their financial information often less common than sophisticated methods. Due to the internet connects the whole countries in the world and Iraqi people like other people in these countries they use the internet to perform their daily transections the same sophisticated methods may be used to obtain the personal information of Iraqi people. In this chapter, the author intends to give the reader an idea about the traditional and non-traditional methods, while in chapter six he will demonstrates whether these methods need to be criminalised in themselves or the criminalising of identity theft will be sufficient to deal with them.

3.1.3 The Illegal Transferring of, Possession of, or Using a Person's Means of Identification

According to some in the academic literature and in regarding to identity theft laws in other jurisdictions, the transferring of, possessing and using another person's means of identification also refers to the illegal act that constitutes the *acus reus* of identity theft.[205] A person is guilty of identity theft if he transfers another person's means of identification, such as giving, selling, or any other act of exchange between other hands rather than remaining in the hands of the authorised person (himself). Possession of another person's means of identification means that the person with this now exercises control over this irrespective of the rights of the person who has a genuine right to use the means of identification. The illegal use of another person's means of identification occurs when the accused has used another person's means of identification to commit other crimes, aid or abet in the commission of these crimes. Literature and jurisdictions that criminalise identity theft do not consider the possession of or the using of another

[205] Identity Theft and Assumption Deterrence Act 1998 1028 a(7) 18 U.S. Code Chapter 47; Identity Theft Enhancement Penalty Act 2004 1028A a(1) PL 108-275 108th Congress 118 Stat. 831, 2004

person's identity as a crime in itself unless the person's identity is used to commit other crimes for illegal ends.[206]

It can be argued that the above illegal activities do not constitute the *actus reus* of identity theft. They constitute *preparatory* activities for commissioning of other crimes or they may constitute elements of another crime that is called 'possession of or using stolen identity'. Neither the literature nor jurisdictions of other States argued this as a crime. They choose not to distinguish between identity theft and the possession of, or using stolen identity, and instead integrate the two types in one term called 'identity theft'. In order to unity the law, the author distinguishes clearly between these two types of crimes, but in his conclusion requests that the Iraqi legislature integrates these two types of crimes and criminalises them under a comprehensive single law. This will be discussed in more detail in chapter six where US identity theft laws are analysed to assess whether or not the Iraqi legislature can adopt or borrow provisions from them.

3.1.4 Participation in Identity Theft

In most legislation the commission of crime may be divided into two types: (1) full commission of crime, and (2) inchoate commission of crime. Therefore, the commission of identity theft may also be divided into two types: (1) full commission of identity theft, and (2) inchoate commission of identity theft or an attempt to commit identity theft. The role of individual perpetrators in committing identity theft may also be different. Some may aid, abet, or conspire with the accused to commit identity theft, while others may steal the means of identification itself.[207] This describes each actor's role in the 'participation' in identity theft. Dependent on the role of the individual perpetrator, participation in identity theft may take the form of principal participation or of accessory participation.

Principal participation means that the accused has committed one or more than one of the elements of identity theft, such as stealing or obtaining another person's means of identification. In addition, a person may be guilty of an identity theft crime (as a

[206] Identity Theft and Assumption Deterrence Act 1998 § 1028 (a) (7); Cheney J S, 'Identity Theft: Do Definitions Still Matter?' (2005) Discussion Paper Payment Credit Card Centre 11 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=815684> accessed on 2 February 2014; S Sproule and N Archer, supra, note1 0

[207] *United States of America v. Shephard*, United States Court of Appeals, No. 10-3215 [8th Cir. 2011] unreported

principal participant) when he uses an innocent agent to commit that crime. Accordingly, he may be regarded as a principal perpetrator, even though he has not presented at the crime scene.[208] While accessory participation means a person or persons may aid, abet, consult, or incite another person to commit identity theft. Perpetrators may also enter into a criminal enterprise to commit identity theft, in a type of participation called 'a conspiracy'. The above types of participation will be illustrated in more detail below.

3.1.4.1 Attempted Identity Theft

Attempted identity theft is an act done with intent to commit a crime of identity theft by the perpetrator, but it unfulfilled, for whatever reason that the perpetrator cannot overcome.[209] Due to Iraq having no specific law deals with identity theft and the attempted identity theft, the general rules that govern other crimes and the attempted of them will be used to explain the attempted identity theft. The Iraqi legislature in section 30 of the Penal Code 1969 defines attempted of crime as the initiation of an act with intent to commit a crime or misdemeanour, if the act has been interrupted or aborted for reasons that the offender cannot overcome.[210] It consists of two elements:[211] (1) act that is committed by the perpetrator, which is called the *actus reus* of the attempted identity theft and (2) the perpetrator's state of mind or what is referred to as the *mens rea* of the attempted identity theft. These two elements will illustrated below.

3.1.4.1.1 *Actus Reus* of Attempted Identity Theft

There are no specific rules that deal with attempted identity neither in Iraq nor in the states that criminalise the theft of a person's means of identification, thus the general

[208] K Hamdorf, 'The Concept of Joint Criminal Enterprise and Domestic Modes of Liability for Parties to a Crime' (2007) Vol. 5 Journal of International Criminal Justice 208-226

[209] New York Penal Law in section 110.00 defines the attempt in a crime as "A person is guilty of an attempt to commit a crime, when, with intent to commit a crime he engages in conduct which tends to effect the commission of such crime. New York Penal Law section 110.00.; the English Criminal Attempt Act Revised of 1981 Section 1 defined the attempt as: attempt to commit an offence: 1 If, with intent to commit an offence to which this section applies, a person does an act which is more than merely preparatory to commission of the offence, he is guilty of attempting to commit the offence, English Criminal Attempt Act Revised of 1981 c. 47

[210] Iraqi Penal Code No. 111, 1969 Section 30

[211] P Marcus, 'Joint criminal Participation Establishing Responsibility, Abandonment Law in U S A Faces Social and Scientific Change, Section V' (1986) Vol. 34 American Journal of Comparative Law Supplement 479-490

rules relate to attempted of other crimes are sometimes used to explain the elements of attempted identity theft.

The *actus reus* of attempted is an illegal activity that is committed by the accused with intent to commit identity theft, but it is not fulfilled for reasons that the accused cannot overcome.[212] The *actus reus* of attempted identity theft should constitute a substantial step in the identity theft occurrence.[213] To accuse a person of attempted identity theft he should initiate to commit one or more of its essential elements or a part of those elements, but he cannot fulfil it for whatever reason. For instance, a person may be guilty of attempted identity theft if he sends bogus emails to trick people into revealing their personal information, even though they do not response to that attempt.

3.1.4.1.2 *Mens Rea* of Attempted Identity Theft

The *mens rea* of attempted identity theft is the perpetrator's state of mind required for him to be guilty of attempted identity theft. The state of mind of the perpetrator means that the criminal should have intent to commit identity theft. In some jurisdictions, (such as US)[214] the intent that is required for this crime is specific intent, because when the perpetrator appropriates another person's information he must intend to use this information to commit other crimes. As a result, the perpetrator should have the knowledge and the purpose to appropriate another person's identity with intent to commit other crimes. In addition, he should know that the person that the means of identification belongs to him does not consent to his information being taken. Furthermore, he should have the knowledge of consequences[215] that may occur if he takes the other persons' information. He should also know that the means of identification that he acquires belongs to another person and is not a false means of identification, and he attempts to obtain it, but he cannot obtain it for whatever reason.[216]

[212] Section 30 of the Iraqi Penal Code, supra
[213] S 5.01 of the American Institute Model Penal Code
[214] Section 1028 (a) (7) Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998)
[215] P Marcus, supra, note 211, 480
[216] There are no rules in Iraq that can be used to define the *mens rea* of attempted identity theft or other crimes. However, scholars have determined this element according to the element of the crime itself. As it was mentioned in chapter four of this thesis, the Iraqi legislature does not define the *mens rea* of theft crime. In addition, there is no literature about attempted identity theft. The author observes that even the US legislature does not provide section neither in the Identity Theft Assumption Deterrence Act 1998 nor

If the previous elements are satisfied, the perpetrator may be guilty of an attempt of identity theft. For instance, the person may be guilty of attempted identity theft if he sends an email to a bank client asking him for more details about his bank account, but the client does not respond to the email and calls the bank to inquire about the legitimacy of the email. The perpetrator may also be guilty of attempted identity theft if he tries to see or hear the person when he gives his information to his bank or his creditor by phone or when he enters his credit card number in an ATM, but he cannot see or hear the information because the victim sees or detects his presence. Graham[217] for instance, observes that in a recent case, the criminal pretended to be PayPal Inc. and sent an email that resembled the PayPal's email to its client. He told client that her account with the payment service provider had become inactive, and it needed to be re-activated. The perpetrator asked the victim to confirm her new email address and other sensitive information, such as her password, credit card data, and PIN of an ATM card. However, the criminal could not gain her information because the alarm bell rang. She alerted the staff of the company and told them of her concern about the illegality of this email.

3.1.4.1.2.1 Recklessness

Recklessness is an element that relates to the *mens rea* of attempted identity theft, but most legislators do not stipulate this in their legislation. The perpetrator may be guilty of attempted identity theft if he recklessly attempts to appropriate information without consent and then use it to commit other crimes, but he cannot fulfil use the means of identification to commit other crimes for whatever reason.[218] He may also be guilty of attempted identity theft if he recklessly attempts to obtain another person's means of identification and gives or sells this to another person who may then use it to commit other crimes. Acting consciously in disregard of the consequences or even the dangers that may occur from using another person's identification without consent, is the state of mind required to satisfy the requirement of recklessness and therefore can be found

the Identity Theft Enhancement Penalty Act 2004 to deal with attempted identity theft. Therefore, the author always refers to what is stated in academic literature about attempted of other crimes and applies it to identity theft.

[217] B Graham, supra, note 147

[218] P Marcus, supra, note 211, 480

guilty of attempted[219] identity theft. If the above element is provided a person may be guilty of attempted[220] identity theft.

3.1.4.2 Accessory Participation

As mentioned previously, participation in the crime is divided into two types: (1) principal participation; and (2) accessory participation. Principal participation in a crime such as identity theft occurs when the perpetrator commits one or all the elements of identity theft, such as sending a bogus email to a person in order to try to trick the victim into divulging information.[221] For example, in a recent case[222], which was stated in U.S. General Account Office Report 2000a, the police caught a principal offender carrying a laptop containing several thousand names, social security numbers and other kinds of private data of over 100 high-ranking United States' military officials. While accessory participation means that the accessory participant does not commit any essential element of identity theft, such as the *actus reus*, he does however, aid, abet or consult the principal participant to commit identity theft.

3.1.4.2.1 Elements of Accessory Participation in Identity Theft

Accessory participation in identity theft consists of two elements: *actus reus* and *mens rea*.

3.1.4.2.1.1 *Actus Reus*

The *actus reus* of accessory participation occurs when the accessory participant participates in committing identity theft by aiding, abetting, instigating or consulting the principal to commit identity theft.[223] If a person contributes to any of the above or consults another person to commit identity theft he may be guilty of accessory participation in identity theft. The general principle is that the accessory participant may

[219] P Marcus, ibid, 480
[220] ibid 480
[221] J J Rusch, 'Making a Federal Case of Identity Theft: the Department of Justice's Role in the Theft Enforcement and Prevention' 2000 available at <http://www.usdoj.gov/criminal/fruad/fedcase_idtheft.html> in G R, Newman and McNally, supra, note 10
[222] U.S. General Account Office (GAO 2002a June), 'Identity Theft: General Awareness and Use of Existing Data Need. Report to the Honorable Sam Johnson, House of Representative Washington, D.C. [G A O-02-766]' available at <http://www.consumer.gov/idtheft/reports/gao-d02766.pdf> accessed on 20 December 2011
[223] *United States v. Wallace L. Lawrence*, supra

not be deemed guilty of accessory participation, if the principal perpetrator does not commit identity theft that the accessory participant aids or abets in. For instance, if someone gives another person an iPhone to take an overt photograph when the targeted person enters his credit card number in an ATM, however the factor uses his iPhone to take the image or he obtains the information by another way. In this instance, the accessory participant may not be guilty of the accessory participation in identity theft.[224] Furthermore, the accessory participant may not be guilty of participation in identity theft if he may make an exchange in an ATM slot, or put a small apparatus to copy the customer's information, but the principal perpetrator obtains the customer's information by other means, or he abandons the commission of identity theft.

According to the Iraqi Penal Code 1969,[225] the principal participant concept encompasses all perpetrators who participate in the commission of a crime, regardless of whether or not they are principals or accessories who assist in the crime by aiding, abetting, consulting or any other means if they are present at the crime scene. For example, a person is considered guilty of being the principal participant in an identity theft offence if he gives a camera to the perpetrator who will intend to use it to take a snapshot of a person entering his PIN into an ATM, and he is present at the process of the taking of the photographic image. However, both the Model Penal Code and the United Kingdom Criminal Penal take a different view from Iraqi legislation in not considering the person who assists in the crime, he being present at the crime scene as a principal perpetrator.

It will be recognised that although the US legislature does not criminalise the taking of a person's means of identification, it does not distinguish between all parties involved in the identity theft offence, whether they be principal or accessory participants treating them together as principal perpetrators in identity theft.

[224] D Lanham, 'Accomplices, Principals, and Causation' (1979) Vol. 12 Melbourne University Law Review 490-515

[225] Ss 47, 48 and 49 of the Iraqi Penal Code No. 111, 1969 deal with participation in the crime; S 47 defines the principal participants in the crime, while s 48 defines the secondary participants in the crime. On other hands, S 49 considers the secondary participant of the crime as a principal participant if he attends at the scene of the commission of that crime. According to this section, a person is considered guilty as a principal factor of crime if he aids, abets or counsels another person to commit a crime and then attends at the scene of its commission.

In the United Kingdom there is no specific law governing identity theft and participation in it, therefore, UK courts may rely upon the s 8 of the Accessories and Abettors Act 1861[226] to cover participation in *identity theft*. Ormerod[227] points out that the language of this Act is archaic, aiding to the ambiguity and inaccessibility the Act. It does not demonstrate the degree of assistance that constitutes the element of accessory participation and in addition does not determine when the person must be convicted of assisting another person to commit a crime; and this introduces some difficulties of interpretation to the courts. In fact, as it will be observed there is no precedent case that deals with identity theft as an actual crime in UK. However, if it is assumed that the UK courts deal with identity theft as an actual crime they do not consider the mere attendance of an accessory participant at a scene of *identity theft* sufficient by itself to make him guilty of participation in *identity theft*. For this, he must have effectively contributed in encouraging, aiding or assisting the criminal to commit *identity theft*.[228]

It is argued that legislators in most countries of the world may determine only the common conduct that may constitute the element of accessory participation, and leave the details to their courts.[229] Therefore, in many cases, the US courts may consider a person guilty of assistance in the commissioning of *identity theft* if he undertook sufficient acts,[230] such as providing a device, a plan, a camera, or lending a laptop to the principal participant in order to send a bogus email to the victim.[231] There is no requirement to prove a causal link between the different types of accessory participation (such as aiding, abetting, or incitement) and the principal crime. It is sufficient to prove,

---

[226] S 8 of Accessories and Abettors Act 1861 UK c. 94, it is stated in this section: (w)hosever shall aid, abet, counsel, or procure the commission of [any indictable offence] 1 whether the same be [an offence] at common law or by virtue of any Act passed or to be passed, shall be liable to be tried, indicted, and punished as a principle offender.

[227] D Ormerod, *Criminal Law, Cases and Materials* (10th edn Oxford University Press New York 2009) 306

[228] *R v Allan* [1963] 2 All ER 897, Court of Criminal Appeal; *R v Clarkson and Carroll* [1971] 3 All ER 344, Courts-Martial Court

[229] For example, the Iraqi legislature states in section 48 of the Penal Code that a person is guilty if he 1. With his knowledge He incites another person to commit crime and the crime is committed accordance to that incitement, 2. He agrees with another to commit crime and the crime is committed according this agreement, or 3. He gives a weapon, or any other thing that may be used to commit the crime, or he aids or facilitates in any way in actions that provide, facilitate or complete the commission of it.

[230] P Marcus, supra, note 211, 483

[231] *United States of America v. Lawrence*, supra, note ; *United States v. Lyons*, United States Court of Appeals, No. 07-3216 [8th Cir. 2009] unreported; United States of *America v. Bell*, United States District Court, Pennsylvania, No. 09-672 [2011] unreported

whether in US, UK, or in Iraq courts, only that aiding, abetting or incitement *facilitates* the commission of *identity theft*.[232]

Occasionally, there is no material evidence aiding or abetting on which the court may depend to prove accessory participation in identity theft. However, commission of identity theft may be surrounded by some circumstances that might be used to refer to the accused as being an accessory participant in identity theft. A court in any jurisdiction in the world has discretion to examine the acts that may constitute assistance in the commission of *identity theft*, and then decides whether a person is guilty of participation in *identity theft*.[233] For example, the court should not depend merely on the presence of a person at the crime scene or his knowledge about the role of the defendant as evidence on his own participation in *identity theft*.[234]

If a court whether in US, UK, or in Iraq provides that the accessory participant is guilty of participating in identity theft, he will be punished with an appropriate punishment as dictated by law.[235] In addition, he may be found guilty of every offence committed by the principal, related to identity theft. For example, if the accessory participant gives the defendant information that the victim would be away and that his private details and personal information might be found in his absence in his bedroom, the accessory participant may then be guilty of participation in any crime that may be committed. In this case, if the defendant went to the victim's house with intention of stealing private information and found the victim not away but at home and the intended victim attempted to catch and detain him, but the defendant shot the victim and killed him, the accessory participant may in this circumstance be found guilty of murder because this

[232] As the author stated in previous footnote there are no rules govern participation in identity theft, he attempts to apply the general rules of participation in other crimes to participation in identity theft. He also attempts to illustrate the elements of participation in identity theft according to literature about participation in other crimes. Therefore he depends on this literature to demonstrate it. K Hamdorf, supra, note 208; M J Allen, *Textbook on Criminal Law* (8th edn, Oxford, Oxford University Press 2005) 201; D Ormerod, *Smith and Hogan*, *Criminal Law* (12th edn Oxford University Press 2008) 172

[233] P Marcus, supra, note 211, 484

[234] See the court decisions in cases *United States v. Garguilo*, 310 F .2d 249, 254 (2d Cir. 1962); *Rv.Bryce*, (2004) EWCA crime 1231 and crime (2004) LR 936

[235] *United States of America v. Oliver*, United States Court of Appeals, No. 09-10133 [5th Cir. 2011]; according to UK and Iraqi legislation the accessory participant is punished as a principal of identity theft, s 8 of Accessories and Abettors Act 1861; s 50 Iraqi Penal Code 111, 1969, whoever participates in the commissioning of a crime whether as a principal factor or a secondary participant they are to be punished by the consequence that is stated to this crime.

unlawful act 'murder' enters within the scope of the potential consequence.[236] However, if the act that has been committed by one of the gang members was completely unconnected to any acts that the other members foresaw[237] they might not be guilty of that act.

3.1.4.2.1.2 The Accessory Participant's State of Mind

The accessory participant's state of mind (*mens rea*) in this context refers to a person(s) who participates, assists or facilitates the commissioning of identity theft crime.[238] This implies that an accessory participant(s) in an identity theft crime has not only an adequate knowledge of the crime, but is also aware of the crime implication.[239] For instance, individuals working in businesses, internet cafes, or any other legitimate engagement may be found guilty of participating in identity theft if such person(s) consciously and knowingly sells or gives the personal information of another person to other people who may use it to commit other crimes. Swartz [240] states, for instance, that some internet websites might sell individuals' bank accounts to any person for a small cost.

The *mens rea* of an accessory participant also means that the accessory participant knows the consequences of his/her role in the commission of identity theft; assisting the commissioning of an unlawful act. Moreover, accessory participants must know the essential elements of *identity theft*, but not all details.[241] However, some jurisdictions d\o not consider the accessory participant in *identity theft* as guilty of participation in *identity theft*, as he/she may not be fully aware of certain details regarding the commissioning of the act - the date and place the crime is committed.[242]

---

[236] *Michigan v. Poplar*, 173, N, W. 2d 732 (1969); J C Smith, 'Criminal liability of Accessories: Law and Law Reform' (1997) 113 Law Quarterly Review 453-467; K Hamdorf, supra, note 208

[237] Allen, supra, note 232, 215; M T Molan, *Cases G Materials on criminal law* (3rd edn London: Cavendish 2005) 340; D Ormerod, supra, note 232, 193

[238] D Ormerod, *Smith and Hogan's Criminal Law* (13th edn Oxford University Press 2011) 201

[239] *United States of America v. Damache*, United States District Court for Eastern District of Pennsylvania, No. 11-420 [2011] unreported

[240] N Swartz, 'Want the CIA Director's Address? Get It for $26 Online' (2003) Vol.37 (6) Information Management Journal, 16 in G R Newman and McNally, supra, note 11 , 27

[241] *Johnson v. Youden* (1950)1 All ER 300

[242] D Ormerod, supra, note 238, 206

The accessory participant may be guilty of being accessory if he knows that he is participating in the commission of identity theft.[243] One other argument against accessory participant in identity theft crime is that if the accessory participant does not intend to assist or encourage the principal perpetrator to commit,[244] and thus may not be guilty of participating in identity theft. An accessory may not also be found guilty of participating in identity theft if s/he has no idea about its essential elements.

A person may be found guilty of accessory participation in *identity theft* if he recklessly aided or abetted a defendant to commit an identity theft offence. Recklessness is a situation in which a person directly or indirectly caused the commissioning of an identity theft crime. It includes actions such as unconscionable support, aiding, encouragement, and abetting other persons, without intention to commit these types of act.[245] However, an accessory participant in this context (recklessness) is fully aware that the act is prohibited, and thus if s/he is unaware that the act is punishable s/he may not be guilty of accessory participating in identity theft.[246]

In summary, there is a difference between the principal perpetrator and accessory participant. A principal perpetrator is a person who commits the act that constitutes an essential element of identity theft (such as the *actus reus* of it), while the accessory participant is a person who assists, encourages, or assists the principal perpetrator in the commission of identity theft. The principal perpetrator may not be able commit identity theft without the assistance of the accessory participant, or he commits it, but using another methods.

However, the situation is different if the perpetrator who commits identity theft via an innocent agent, such as an infant, an insane person or someone who lacks *mens rea*. In this case, in spite of the perpetrator does not attend at the scene of the commission of *identity theft* or commit an essential element of it, such as the *actus reus* he may be

---

[243] W Wilson, *Criminal law: Doctrine and Theory*, (2nd edn London: Longman 2003) 595

[244] The Law Commission, Law Com No 305, Participation in Crime, Presented to the Parliament of the United Kingdom by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty 2007 available at <http://lawcommission.justice.gov.uk/docs/lc305_Participating_in_Crime_report.pdf> accessed on 20 December 2011

[245] A Reed and B Fitzpatrick, *Criminal Law* (4th edn Sweet and Maxwell 2009) 68; AP Simester, J R Spencer, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law, Theory and Doctrine* (4th edn Oxford and Portland, Oregon 2010) 140

[246] D Ormerod , Smith& Hogan, supra, note 232, 195

regarded as a principal perpetrator of identity theft.[247] According to the principle of legality and the definition of *identity theft* a person is guilty of *identity theft* if he commits the *actus reus* of identity theft or any essential element of it. For instance, if a person takes another person's means of identification he is guilty of identity theft because he commits the *actus reus* of identity theft. In the above case, the insane person or the person who lacks the *mens rea* commits the *actus reus* of identity theft when they take another person's personal information, while the genuine criminal does not commit the *actus reus* and he is not at the scene of the crime when the information has been taken. Thus, the insane person should be guilty of identity theft, but because he is an insane person lacking the *mens rea* he cannot be guilty of identity theft. However, in order to protect people and their properties the Iraqi legislature accepts this case from general role and accuses the genuine criminal of *identity theft* even if he does not commit the *actus reus* of identity theft or any essential part of it, or does not attend the scene of the commission of crime and considers him as guilty of crime.[248]

3.1.4.3 Conspiracy in the Identity Theft

Identity theft may be carried out by an individual or a group of persons. Occasionally, individuals may make an agreement among them to carry out identity theft, as it is a complex crime and may sometimes require more than one person, particularly if it is committed online. Accordingly, the commission of identity requires huge skill, experience, and capability. Some forms of identity theft, especially online identity theft, can consist of a range of activities that require more than one person to be accomplished,[249] thus it requires a high level knowledge or experience in the use of computers and the internet. The perpetrator, for example, may sometimes take many steps before committing an identity theft. He may look for soft target, identify the way to access the information of the target, or gain the essential documents, regardless of whether they are legitimate or counterfeit to institute authenticity. Thereafter, he chooses the way that may be used to exploit or obtain identity of victim in order to commit other crimes. It may involve but not limited to open a new account, perpetuate

[247] D Ormerod , Smith& Hogan, supra, note 232, 198; K Homdorf, supra, note 208, 219; Allen, supra, note 232, 198

[248] The Iraqi legislature states in section 47 (3) of the Penal Code 111 that a person is guilty of crime if he induces another person to commit the *actus reus* of that crime if that person is irresponsible of being guilty of crime; D Ormerod, supra, note 227, 297

[249] G R Newman and M M McNally, supra, note 11, 5

existing account, or persuade the officers that the documents belong to the person who is named.[250] All these steps may require more than one person to be fulfilled. As a result, the perpetrator will search for other perpetrators to assist him. If he agrees with those perpetrators to commit identity theft, a conspiracy to commit identity theft may be established.

A conspiracy is an agreement between two or more two persons with intent to commit identity theft.[251] For instance, it was stated that in 2002, a criminal gang in US stole social security numbers and other credit card data from 80 deceased persons across five states in the United States. The gang sold the information for $600 per name, to individuals who in turn, use it to process car loans.[252] In addition, it has been reported that some of the persons accused in the 11 September bombings in US were involved in identity theft.[253]

The difference between conspiracy and being an accomplice seems to be apparent, as conspiracy requires an agreement between the participants who are involved in the *identity theft*, while there is no an agreement in the accomplice. In addition, the state of mind of participants in conspiracy is divided into two parts: (1) a participant must have an intention to enter into an agreement with the other participants and (2) he must have an intention and knowledge that *identity theft* shall be carried out as a result to this agreement.[254]

3.1.4.3.1 Elements of Conspiracy

There are two elements of conspiracy: (1) an agreement among the participants and (2) the participants' state of mind.[255]

[250] G R Newman and M M McNally, supra, note 11, 5
[251] *United States of America v. Abullatif Jabi*, United States Court of Appeals, No. 90-3643 [6th Cir. 2011] unreported; *United States of America v. Karen Clark*, United States Court of Appeals, (11th Cir. No. 10-10801 [2011] unreported
[252] Techniques of Identity Theft, CIPPIC Working Paper No. 2 (ID Theft Series), 2007, 1-39 available at <https://www.cippic.ca/sites/default/files/IDT_No.2-Techniques.pdf > accessed on 9 May 2014
[253] N A., Jr. Willox and T M Regan, 'Identity Fraud: Providing a Solution' (2002) Vol.1 (1) Journal of Economic Crime Management 1-15
[254] P Marcus, supra, note 211, 485
[255] ibid 485

3.1.4.3.1.1 An Agreement among Participants

A conspiracy in identity theft requires an agreement among the participants to commit identity theft.[256] The agreement is considered to be the heart of the conspiracy. If there is no agreement among the participants to commit identity theft, there is no conspiracy.[257] The agreement may not necessarily be a real agreement, therefore, the defendant may be guilty of conspiracy of identity theft, and even if the other participants are not seriously committed their agreement or they have no intention to commit identity theft. For example, a secret police officer or a person who works as a spy for the police may agree with other persons to commit identity theft, but in reality may not fulfil the agreement, thus instead he may betray or breach the agreement by facilitating the arrest of other participants. Consequently, if the identity theft is committed the other accomplices may be found guilty of conspiracy in identity theft. This type of agreement is called a "unilateral approach." A court in "unilateral approach" agreement focusses on the element of mental state of the participants, to decide whether a person is guilty of conspiracy and ignores the fact of the agreement.[258]

When persons consciously agreed to commit an identity theft crime, those persons may be found guilty of conspiracy in *identity theft* regardless of their role. Conspiracy in an act of an *identity theft* offence is committed even when culprits do not know each other.[259] In their article, Newman and McNally[260] observe a case that may be an example on a conspiracy in an identity theft offence. In this case, from between 1999 and August 2000, a criminal work as a help-desk worker at Teledata Communications, Inc. - a Long Island Computer Software Company that gave banks computerised admission to databases containing credit data, stole huge amount of individuals' information and then sold it to his accomplices. In addition, he stole ten thousands of credit reports and sold each report for $30. Subsequently, the information was

[256] *United States of America v. T Kasenge*, United States Court of Appeals, (1st Cir. [2011]) unreported
[257] P Marcus, supra, note 211, 485.
[258] *Minnesota v. St. Christopher* 232 N.W .2d 789 (1975)
[259] *United States v. Bruno* 105 F .2d 921 (2d Cir. 1939), rev'd on other grounds, 308 U.S. 281
[260] GR Newman M M McNally, supra, note 11, 97

distributed to roughly 20 accomplices, who in turn, sold it to a network of perpetrators. In this case, the help-desk worker was accused of conspiracy. [261]

Occasionally, organised crime gang members connive with officials or workers in an organisation or company, such as a restaurant or a petrol station to steal people's means of identification. In addition, they may agree with officials at the internet sites to skim the credit cards or debit cards details of customers when they use the internet to sell or purchase goods.[262]

3.1.4.3.1.2 The Element of Mental State of Conspirator - the Participant of Identity Theft

The element of mental state of a conspirator consists of two parts; (1) the intention or desire to engage other participants to commit identity theft crime and; (2) the intention or action which shows that identity theft crime shall or about to occur resulting from agreement with other participants.[263]

If the participant has an intention to enter into an agreement with other persons to commit identity theft and he has an intention that the identity theft shall be committed as a result to this agreement he may be found guilty of conspiracy in identity theft.[264] However, courts may face difficulties in proving these two parts of the element of mental state of conspiracy. As a result, the *court*, depends on its jurisdiction, may infer the elements of mental state of conspiracy from the circumstances of the evidence.[265]

If an identity theft crime has been committed based on the conspired agreement by participants, parties to such agreement may be found guilty of both conspiracy and identity theft. In this point, conspiracy is distinguished from attempted identity theft.

---

[261] *United States of America v. Philip Cummings*1:03-cr-00109-gbd-1 (2004), on September 14, 2004, the criminal pled guilty of three account: (1) conspiracy to defraud the United States; (2) fraud by wire, and (3) fraud with documents. He was sentenced to 5 years in prison on account one, 14 years in prison on second account, 14 years on third account, and 3 years of supervised release. The prison terms are to be served concurrently with each other. In addition, he was sentenced to $ 15, 386,673 in restitution.

[262] Newman and McNally added that criminal gangs agreed with workers at restaurants to skim credit card or debit card information of clients and send it to them. They paid fees to each credit card or debit card details, GR Newman M M McNally, supra, note 11

[263] *United States of America v. Gonzales*, United States District Court, District of New Jersey, No. 09-18 U.S.C. §371 and 1349 [2009] unreported

[264] *United States of America v. Berdize*, United States Court of Appeals, No. 10-0064 Cr, [2nd Cir. 2011] unreported

[265] *Direct Sales Co. v. United States* 319 U. S 703(1943)

Attempted identity theft combines with identity theft when it has been committed. Defendants in attempted identity theft may be convicted of identity theft only while they in conspiracy of identity theft may be convicted of both conspiracy and identity theft. Perpetrators in conspiracy of identity theft may also receive consecutive sentence.

As in the attempt and the accomplice in an identity theft crime, participants in the conspiracy of identity theft may be found guilty for each crime that may be committed by any member of the gangs, as long as it could be reasonably anticipated as a necessary or probable outcome for the illegal agreement among them.[266] It was stated in *Pin Kenton v. United States*[267] that every participant might be guilty of the probable consequence, even if the consequence was not discussed in the agreement that has been held beforehand or intended by the participants.

In *R v Powell and English*, the British House of Lords outline required conditions that are to be considered for participants in a joint criminal venture, which are liable for any act that has been committed by a member of the venture. The House of Lords stated that participants may be guilty of illegal activities that are committed during fulfilment the agreement if they foresaw or contemplated an act as a possible crime.[268] Consequently, it is sufficient for each participant in a joint criminal venture, such as identity theft crime, to be liable for any act that was conducted by other perpetrators, if he foresaw, or contemplated that the act might occur.

Nowadays, conspiracy in identity theft is widespread in most countries across the world. For instance, a number of criminal gang organisations in South Asia use stolen identities to produce plastic cards that have been sold on the street in many cities of United States and Europe.[269] To avoid the detection, they use highly complicated methods to store the data of credit cards or transfer it. They may work in small groups, deal with huge size, and work in a high-populace region. They commit identity theft in an area, which is frequently far from their home.[270]

---

[266] B Krebs, 'Joint Criminal Enterprise' (2010) Vol. 73 (4) The Modern Law Review 578
[267] *Pin Kenton v. United States* 328, U.S. 640 (1946)
[268] *R v Powell and English*, (1999), 1 AC1 (HL)
[269] J Newton, Det. Chief Insp, *Organized Plastic Counterfeiting*, London, (Home Office 1994), cited in G R Newman and M M McNally, supra, note 11, 6
[270] F Motivate and p Tremblay, 'Counterfeiting Credit Cards: Displacement Effects, Suitable Offenders, Crime Waves Patterns' (1997) Vol. 37 (2) British Journal of Criminology 165-183

In effect, the expansion of unlawful activities that relate to identity theft in the world is unknown,[271] because of globalisation and the increase in the use of credit and debit card. In addition, the vulnerability that may be found in the international system of card verification and the delivery may be exploited by criminals to commit identity theft.[272] Some officers in Postal Inspection Service of U.S also reported an increase in organised crime gangs involving identity theft.[273] It might be argued that conspiring in identity theft is seemed to be more dangerous than participation in identity theft itself. This means countries' domestic criminal laws are inadequate to combat it, as it requires cooperation between countries and agencies across the globe.

3.2 Defining Identity or Means of Identification

Identity or another person's means of identification is the main element that may cause legal challenges. It is a complex and ambiguous term[274]; and as a result, there is no definitive definition for it. Before defining 'identity' in academic terms, one should perhaps first refer to a dictionary definition. 'Identity' in general, means 'the sameness of a person or thing at all times or in all circumstances. It is the condition or fact that a person or thing is itself and not something else, such as individuality or personality.'[275]

It is easy to apply the above definition to certain identities, but it may not be socially applied to other identities, such as 'national identity' because the reality and situation of 'being' are the same for all nations and does not differ; the only thing that differs is the *content* of differences between nations. In the Oxford English Dictionary, 'identity' can also mean 'the set of behaviour or personal characteristics by which an individual is recognised'.[276]

In the literature, identity is defined in many ways, such as a person's concepts, opinions, what they are, what sort of people they are, or how they relate to one

---

[271] G R Newman and R Clarke, *Superhighway robbery: Preventing e-commerce crime* (London: Willan, 2003) 6
[272] ibid, 6
[273] G R Newman and M M McNally, supra, note 11, 26
[274] James D, Fearon, 'What is Identity (As We Now Use the Word)' 1999, 1 available at <http://www.stanford.edu/~jfearon/papers/iden1v2.pdf > viewed on 30 March 2012
[275] Oxford English Dictionary, (2nd edn 1989); Merriam-Webster Online Dictionary available at <http/www.m-w.comdictionary/identity> viewed on Jul 25, 2010
[276] Oxford English Dictionary, ibid

another.[277] It can also mean characterising the way in which people and entities, such as countries or nations can define themselves or the way by which one recognised, for example, by race; ethnicity; religion; language and culture.[278] Jenkins[279]defines identity as the method by which people and groups can be distinguished in social setting. In addition, identity is defined as a condition in which a population of individuals has the same identification with national symbols – internalized the symbols of nations'.[280] It has been stated that identity are vectors that are acquired to obtain identities relatively stable, role, specific understanding, and expectation about self by participating in collectives.[281] Thus, Wendt[282] defines social identities as:

> [A]re sets of meanings that an actor attributes to itself while taking the perspective of others, that is, as a social object. ... [Social identities are] at one cognitive schemas that enable an actor to determine `who I am/we are' in a situation and positions in a social role structure of shared understandings and expectations

Identity is used in different fields to distinguish individuals each other, to describe the relationship between the individuals and the State or to describe a specific group. As a result, it has different names, such as gender identity, personal, national, and ethnic identity. It has also many elements and different structure. Scholars, as well, use the identity term to express many things, so it has different elements and structure. However, it can be used to refer to two main things that always are used between academics and individuals: national identity and personal identity.[283] The main concept of identity that concerns this study is the personal identity or a person's means of identification. Personal identity or a means of identification can be used to identify an individual.

A suitable definition of personal identity or a means of identification of a person is the definition that is set forth in the Identity Theft and Assumption Deterrence Act of 1998 of United States. In this Act, the United States legislature defines personal identity as:

---

[277] M Hogg and D Abrams, *Social identification: A Social Psychology of Intergroup Relations and Group Processes*, (1st edn, Routledg London: 1988) 2

[278] F Deng, *War of Vision Conflict of Identities in the Sudan*, (Washington DC: Brooking 1995), 1

[279] R Jenkins, 'Categorization: Identity, Social Process and Epistemology' (2000) Vol. 48 (3) Current Sociology 7-25

[280] W Bloom, *Personal Identity, National Identity and International Relations* (Cambridge Cob. V Press 1992) 52

[281] A Wendt, 'Anarchy Is What State Make of It' (1992) Vol. 46 (2) International Organizations 391-426

[282] A Wendt, 'Collective Identity Formation and the International State' (1994) Vol. 88 (2) American Political Science Review 384-396 as seen in J D Fearon, supra, note 274

[283] R Jenkins, Categorization, supra, note 279

'any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual'.[284] It could be said that this definition does not refer to the main subject of identity theft because as it was noted in the previous chapter; criminals do not target individuals only. They target individuals, companies, institutions of State or any other entity that may benefit from using its identity. Therefore, personal identity or a means of identification can be defined as any information whether biological or physiological, such as a finger print, voice print, retina or iris image, deoxyribonucleic acid DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit and debit cards numbers, financial institution account number, passport number, password and driver licence number that is usually used alone or combination with other information to identify or purport to identity a person.

The identity or means of identification has become more important in current life. Individuals have a right to use multiple means of identification to define themselves. It consists of many elements, such as names, addresses or any other sensitive information. In effect, people often use their names as means to identify themselves. However, if they use their names as means of identifications that may raise many problems because most people have the same names, as a result, it is very difficult to make distinguishing between them by using names only. In addition, some people in their lives use more than one name and that may make the discrimination between them by names impossible. Consequently, people should use another element with their names to enhance it, such as social security number, password, or driving license number. Personal identity or a means of identification of another person has become more susceptible to risk and misuse by unscrupulous people.

If a person uses a means of identification, such as a name, address, or driving license number alone or in conjunction with any other information, to define himself, he has authority to use it and to prevent another person from using it, without his consent. In other words, as some scholars[285] observe, the means of identification that is used by the person to identify himself belongs to that person, and taking it without his consent

[284] S (c) (3) (C) Identity Theft and Assumption Deterrence Act of 1998 USA, supra

[285] Interview with Professor Dr. Murhij specialist in criminal law, Anbar University, School of Law, (Anbar, 20 January 2013); Dr. Alaa Baaj Specialist in criminal law and a lecturer at School of law, Baghdad University, School of Law (Baghdad, 30 January 2013)

should constitute an offence.

3.2.1 Belonging to Another

A means of identification, such as a passport, credit card number, mother's maiden name, social security number, and PIN number as an object of theft, should belong to the person owns or who has the authority to use it. Therefore, if it has not been acquired by another person it is considered 'an abandoned means' or it is a false means of identification. Consequently, if this means of identification is taken by a third person he himself may not be guilty of identity theft. However, he may be guilty of fraud if he uses the false or abandoned means to obtain another person's property.

3.3 *Mens Rea*

Although the *mens rea* is considered to be the core element of identity theft most legislation that criminalises the use of a means of identification of another person without his consent does not precisely determine the concept of it.[286] Generally, *mens rea* consists of two core elements: (1) knowingly and willingly and dishonesty taking another person's means of identification, and (2) the intention to use this means of identification to commit other crimes. These elements will be discussed in detail below.

3.3.1 Knowingly and Willingly and Dishonesty Taking Another Person's Means of Identification

As mentioned previously, Iraq has no specific law to deal with identity theft crime. Therefore, to determine the elements of *mens rea,* one has to return to general rules related to *mens rea,* drawing from the UK and US experience to determine the elements of *mens rea*.

According to Iraqi general rules, the *mens rea* of a crime consists of two elements; knowing and wilful. 'Knowing' means that the accused should know that he takes and uses another person's means of identification and has knowledge the person does not accept his means of identification being taken. If the accused does not know that he has taken or used another person's means of identification or believes that that person accepts to his means of identification is being taken he may not be guilty of identity

[286] Section 7(a) of Identity Theft and Assumption Deterrence Act 1998 U.S

theft. He should also know that the means of identification belongs to a person whether the person is dead or alive. In addition, he should know it is not a false or an abandoned means of identification. Taking another person's means of identification should be intentionally. If an accused innocently or mistakenly takes and uses another person's means of identification he may not be guilty of identity theft.

Identity theft in the UK is not handled as a separate crime, and thus there is no specific law to deal with it.[287] However, the term dishonesty is stated in the UK's Theft Act of 1968. As the concept of dishonesty is stated in the UK's Theft Act 1968, it applies that an act of identity theft is also considered to be an act of theft. It means taking another person's means of identification without his consent and without a right to use such information constitutes an act of theft. To determine whether an accused is guilty of identity theft, courts in the United Kingdom use two standards (common and accused judgment) to decide whether the defendant's conduct is dishonest or not. Common standard is determined by a deferent person who is in the same conditions with the accused. This standard is based on an answer or confession from the accused through responding to question; 'which the accused commit 'dishonest by common standards?' If the answer is 'yes,' the defendant may be guilty of identity theft, however if the answer is 'no,' the defendant may not be guilty of identity theft. The second standard is the accused's judgment or what the accused believes, in this standard, the courts ask the question: whether the accused believes in what he did as 'dishonest' by the common standards? If the answer is 'yes' the accused may be guilty of identity theft. However, if the answer is "no" the accused may not be guilty of identity theft.[288]

Courts should deal cautiously with these standards. They should not take any of them and absolutely apply it to the accused. Courts for instance, should not take the common standards and apply it to the accused without taking into account the accused's belief. On the other hand, they should not take the accused's belief and apply it alone without taking into account the common standards. Accordingly, the reasonable solution is the court should make a balance between the two standards to take a reasonable decision. Exceptions that are mentioned in the Theft Act of 1968 confirm that. The person for

[287] Cabinet Office, 'Identity Fraud: A Study' 2002, 3-5 available at <http://www.statewatch.org/news/2004/may/id-fraud-report.pdf> accessed on 19 July 2011

[288] K Campbell, 'The Test of Dishonesty in *R .v. Ghosh*' (1984) Vol. 43 Cambridge Law Journal 349-360

instance, may not be found guilty of identity theft and his act is honest if he believes when he/she appropriates another person's means of identification (such as a password, social security number, or credit card number) that he has a right in law to take this information.[289] The person's belief makes the act that it is conducted by him, honest and s/he may not be guilty of identity theft regardless of the belief was reasonable or not. Nevertheless, if the person's belief is merely a moral right, the person's act will be dishonest because the belief[290] in the moral right will not be sufficient and he/she may be guilty of identity theft.

More so, a person may not be guilty of identity theft if s/he believes that the person to whom the means of identification belongs will accept his identification is being taken. A son's act, for example, may not be considered a guilty act, if the son mistakenly believes that his father accepts his social security number is being taken or used.[291] Additionally, a perpetrator may not also be guilty of identity theft if s/he believes that the means of identification does not belong to another person, and/or is an abandoned means of identification. A court might hold that a perpetrator who uses another person's identity is guilty of identity theft, particularly if the perpetrator knows that the identity belongs to another person. Courts, for example, held that it is not enough to prove that the person uses false documents identifiers,[292] the culprit should know that the means of identification belongs to another person who is either dead or alive.[293]

Given the fact that the term 'dishonesty' is nowhere to be found in the Iraqis' theft offence law, the Iraqi legislature is thus require to adopt the term 'dishonesty'. This is with the view of determining whether the accused is guilty of identity theft or not. The Iraqi legislature should define the term 'dishonesty' as precise as possible in order to address the limitations associated with the UK's conceptualisation of dishonesty.

The US legislature tightens the conditions that are required to *mens rea* of identity theft, particularly in the Identity Theft Penalty Enhancement Act of 2004. According to this

---

[289] D Ormerod, *Criminal Law, Cases and Materials* supra, note 227, 780
[290] *Harris v Harrison* [1963] Crim LR497, DC.cf Williams CLGP, 322
[291] D Ormerod, *Smith and Hogan, Criminal Law*, supra, note 232, 780
[292] *United States of America v Roperto Miranda- Lopez*, United States Court of Appeals, No 07-50123 (9th Cir. 2008) unreported; *Flores –Figueroa v United States*, United States Court of Appeals, 129 S Ct 1886(8th Cir. 2009)
[293] *States of Kansas v. Bradly D Hardesty*, Court of Appeal of the States of Kansas, 42 Kan. App. 2d 431 (2009)

Act, a person may be guilty of identity theft, even if s/he uses a means of identification of another person with the person's consent. The *mens rea* of identity theft under this Act consists of 'knowingly and without lawful authority using a means of identification of another person. The United States Court of Appeals, First Circuit in *United Stated v. Ozuna Carbera*[294] construe the term 'without lawful authority' as the use of a means of identification of another person against the law, which constitutes *mens rea* of identity theft, even if the person's consent has been given. The US situation will be discussed in more details in Chapter Six.

3.3.2 Recklessness

Recklessness relates to perpetrator's state of mind. The perpetrator may directly commit identity theft; with criminal intention, criminal liability to commit, or he may recklessly commit identity theft. Recklessness refers to an act that has been conducted by the perpetrator(s) without intention to commit *identity theft*.[295] A person, for instance, may recklessly give personal information of another person to criminal(s) who may in turn use it to commit other crimes. Moreover, the person may recklessly use this means of identification to commit other crimes. The case of recklessness as a part of *mens rea*, which is a requirement for committing an identity theft, is also not found in Iraqi legislation. The Iraq law does not seem to have specific Act which directly deals with identity theft while the traditional theft offence (currently in statutory book) has not adequately explained 'recklessness' in relation to crime committed intentionally.[296] In the UK and US legislations, recklessness is not adequately stated as defined in Canadian legislation. The Canadian law determines the term 'recklessness' as a part of the state of mind of the accused that which is required for committing identity theft.[297] Therefore, any effective means of curbing identity theft, the Iraqi legislature needs to adopt the term 'recklessness' as a part of *mens rea*.

3.3.3 Using Another Person's Means of Identification to Commit Other Crimes

The second element of the *mens rea* or the state of mind of the criminal is the intention

[294] *United States v. Ozuna Carbera*, United States Court of Appeals 663 F. 3d 496 (1st Cr. 2011)
[295] M R Berry, 'Does Delaware's Section 102(b) (7) Protects Reckless Director from Personal Liability? Only if Delaware Courts Act in Good Faith' (2004) Vol. 79 Washington Law Review 1125-1152
[296] Iraqi Penal Code1969 Section 439
[297] Section 10 of Bill 4 2009 Criminal Code of Canada

to use another person's means of identification to commit other crimes. Some jurisdictions have clearly stated that a person is guilty of identity theft if he uses another person's means of identification with the intent to commit other crimes. This implies that a person may not be guilt if s/he does not use this means of identification to commit other crimes.

It could be argued that a means of identification is more important in people live. Nowadays, a person's means of identification can be used in other transactions. This practice is very common, particularly in internet shopping, banks and public institutions using computers. Similarly, criminals and unscrupulous persons have now used the same opportunity to perpetuate their criminal intention. It might be said that taking another person's means of identification without his consent constitutes identity theft even if the accused does not use it to commit other crimes.

3.4 Conclusion

This chapter examined elements of identity theft in relation to contemporary Iraqi legislation as well as the literature and the legislation of other jurisdictions. It was observed that Iraq has no specific law to deal with identity theft. Therefore, these elements have been examined according to the general rules of existing Iraqi theft offence laws, literature and other jurisdictions. It appeared that identity theft as opposed to laws in other jurisdictions (such as US and UK) consists of two main elements: *actus reus* and *mens rea*, however, in Iraq law a subject matter of crimes committed against a person's property (means of identification) constitutes the third element of theft. *Actus reus* of identity theft consists of elements: illegal or legal activity to obtain another person's means of identification, transferring, possession, and using another person's means of identification. The study also showed that identity theft is considered to be a special crime, because it relates to sensitive information. Stealing information requires specific methods (such as phishing, hacking, social engineering and skimming).

Numerous types of non-traditional or sophisticated methods of committing identity theft were explored in this chapter. Some of the methods discussed include malware; viruses; worms; Trojan Horse; phishing and hacking. It was observed that these methods engaged by identity theft criminals could be used in different ways to obtain personal

information. Evidence from the review indicated that most crimes are committed through organisation or individuals' computers. Other mediums through which identity theft are committed are through taking or using customers' identities in the course of commercial activities. In some instances, identity theft criminals intercepted messages sent to customers from their bank accounts or any other entities that they deal with and then change the contents of these messages. Of all the methods of committing identity theft observed, phishing appeared to be the top most commonly used method.

The present study has shown that the internet has many vulnerable areas, which can be exploited by perpetrators to access personal information, and then use this acquisition to commit other crimes. Although companies, service providers and other bodies attempt to give protection to the internet, criminals still continue to develop methods to gain access to personal information and later use it to commit other crimes. Such methods can be used to commit identity theft remotely. Some users remain unaware and do not know what these methods are, and how are they working, and that the criminal accessing then can use them to commit other crimes.

However, traditional methods are increasingly used by criminals to commit identity theft. Many cases mentioned in this chapter suggest that traditional methods are in fact more prevalent than non-traditional methods. The present study has shown that traditional or offline identity theft occurs more often than non-traditional or online identity theft. But there is no study or survey analysis that specifically addresses why traditional or offline identity theft occurs more often than non-traditional or online identity theft. The conclusion is reached that the main reason behind the use of traditional methods over non-traditional methods is due to some criminals being closely connected and trusted (such as former friends, friends, siblings, co-workers, a wife or husband, a lessor) and having easy access to relatively others' information.

In this chapter participation in identity theft has also been brought to the reader's attention because it is considered a more serious issue; particularly as some identity theft crimes may be committed online and need more than one person to commit them. There are a great number of established gangs of an identity theft crime in the world. Participation in identity theft is divided into two types: (1) principal or (2) accessory participation. Identity thieves may be involved in criminal enterprise to commit identity

theft. It has been argued that this type of participation is more dangerous and the criminal domestic law alone cannot fight identity theft. Dealing adequately with identity theft needs world cooperation.

The *mens rea* of identity theft consists of two elements: firstly, knowingly using another person's means of identification and secondly, intending to commit other crimes. With respect to the element of 'knowingly', this study has attempted to discuss the term 'dishonestly' that is stated in the UK's Theft Act 1968. It was revealed that this term is not found in Iraqi legislation. The study argues that the Iraqi legislature ought to adopt it. The instance of 'recklessness' has also been discussed in this study. It was demonstrated that this case is not found in Iraqi legislation nor in UK and US legislations that deal with identity theft. The study suggests that the Iraqi legislature should adopt the term 'recklessness' as an element of *mens rea* of identity theft.

A means of identification is a name or a number that can be used alone or together with other information to recognise and identify a person. This constitutes the third element of identity theft. It is a complex and complicated term. It can be used in different fields. The means of identification to be the subject of theft it should demonstrably belong to another person irrespective of whether or not he is alive or dead. The study discussed that the means of identification of companies, government institutions and other bodies and organisations should also be considered as being vulnerable to identity theft.

In summary, in this chapter, it has exposed that there is no legislation determining what precisely are the elements of identity theft. Even some countries, (such as USA, Canada, or Australia) that have specific laws in place to deal with identity theft do not in fact determine these elements.

Having thus determined the concept of identity theft and its elements, a question still remains if identity theft has happened in Iraq, which has no specific law to curb it, can Iraqi courts apply the current theft offence laws or any other existing laws to fight it and reduce its risks? This issue is discussed in the next chapter.

Chapter Four:

Possible Challenges in the Application of Iraqi Theft Offence Laws to Identity Theft Crimes: The Property Debate

Introduction

It is common knowledge that theft is a crime that damages an individual through loss of property. It consists of two main elements *actus reus* and *mens rea* and a third element the property is referred to as a subject of theft. When the current Iraqi theft offence laws were enacted in 1969, the only movable property was object to theft. The Iraqi legislature did not anticipate that a person's means of identification and their financial information would be subject to theft. Consequently, these laws have been enacted to deal with crimes of theft committed against the movable property, and provided adequate rules to protect it. However, technological development and the need of people's means of identification or their financial information to achieve people's transactions have made it more susceptible to some illegal activities (such as theft). This crime is called identity theft.

As the Iraqi legislature did not envisage that intangible properties, particularly personal and financial information might be subject to such illegal activities, therefore does not provide provisions in theft offence laws to govern these illegal activities. As a result, often, courts encounter some difficulties in applying theft offence laws to redress identity theft crimes (or find a proper legal framework to govern it. The new crime poses three challenges to Iraqi courts when they try to apply theft offence laws to identity theft, whether the means of identification is property, can the courts apply the traditional term 'appropriation' to methods that are used to obtain this means of identification, and finally, is there permanent deprivation to the person of his means of identification.

Thus, in this chapter, crimes of theft will be analysed and discussed in Iraqi legislation to examine whether existing theft offence laws are adequate to govern identity theft offences. In other words, it will be asked whether identity theft falls within the scope of crimes of theft in Iraq. In doing so, the elements (*actus reus* and *mens rea*) of theft offences will be examined in detail. Therefore, the chapter will illustrate the following

points: *Actus reus* and *mens rea* of theft offences. In addition, it will discuss the property as a subject matter of theft. The author will also propose potential *actus reus* of identity theft.

4.1 Difficulties That Are Caused by *Actus Reus* of Theft

In this section the general conception of *actus reus* of theft offences in existing Iraqi theft offence laws and the challenges (can personal information be subject to physical theft and, is personal information property), that may be faced when these laws are applied to identity theft will be discussed.

4.1.1 General Conception of *Actus Reus*

The term *actus reus* derives from the Latin expression for "guilty act"; it refers to the external or objective element of a crime. When *actus reus* is proved beyond a reasonable doubt combined with *mens rea*, or so called 'guilty mind', this produces criminal liability in common and civil law jurisdictions. In the section 439 of theft offence laws, The Iraqi legislature uses the term 'appropriation' to refer to the guilty act or so called *actus reus*.

The element of *actus reus* or appropriation may pose challenges or difficulties to the Iraqi courts when they apply the current theft offence laws to identity theft. Therefore, it is necessary in this section analysing this element to examine challenges that may be faced when existing Iraqi theft offence laws are applied to identity theft. In other words, analysing the element of appropriation to examine whether the misuse of personal information falls within the scope of theft offences in Iraq or not.

4.1.2 Challenges of Applying the Term Appropriation to Identity Theft

Here, the general definition of the term 'appropriation' will be discussed before examining the challenges or the difficulties that may be caused by applying the Iraqi theft offence laws to a person who commits identity theft.

4.1.2.2 Definition of Appropriation of Traditional Theft Offences

Literally, the term appropriation is derived from the Latin '*-appropriare-*'. It refers to 'to make one's own', or 'to set aside'. The Iraqi legislator does not define the term

'appropriation' in the current Iraqi theft offence laws 1969,[1] where jurisprudence adopts two theories to define it. These theories are Jarraud's and Garson's theories. Jarraud's theory is based on the assumption that appropriation takes place when the perpetrator takes or carries away the property of another person without his or her consent. According to this theory, the appropriation occurs only when there is taking or carrying of another person's property away. It needs to physical movement.

Garson, in his theory agrees with Jarraud that appropriation occurs when the accused takes or carries away another person's property, but he goes further and distinguishes between the types of possession of property. He states that there are three types of possession: (1) full possession, (2) incomplete possession and (3) incidental possession.[2] According to these types of possession, the term 'appropriation' will be defined and determined as an element of theft. For instance, if a person has the full possession or incomplete possession and takes the property he is not guilty of theft because in full possession the person takes his own property whereas in incomplete possession, the property is already in his possession and he does not take or carry it away. However, if the person has incidental possession and takes the property away he may be guilty of theft. For example, if X gives Z his watch to repair, but Z refuses to return it to X; then Z may be guilty of theft.

Appropriation is also means the act of setting aside something to apply it to a particular usage, to the exclusion of all other uses it. It means that a person who commits theft deals with the thing as his or her own regardless of the owner's rights.[3] However, the UK legislature defines the term 'appropriation' as:

> [A]ny assumption by a person of the rights of an owner amounts to an appropriation, and this includes, where he has come by the property (innocently or not) without stealing it, any later assumption of a right to it by keeping or

[1] Section 439 of the Iraqi Penal Code No. 111, 1969

[2] Full possession means that a person has the two elements of possession of the property (the corporeal and the moral). For instance, if someone buys a car or a house, he or she becomes the owner of that car or the house, and he or she has full possession; incomplete possession occurs when the possessor has only the corporeal element of possession and the moral element remains with the owner of the thing. This type of possession happens through trust contracts such as tenancy, loans, and fiduciary; Temporary possession occurs when the owner hands his/her property over to another to see it, check, or assess its value and then returns it to him/her. In other words, it is the state in which another person's property may be found between the hands of the accused without any authority of it.

[3] R Heaton, *Criminal Law*, (2nd edn Oxford University Press 2009) 277

dealing with it as owner.[4]

In the Model Penal Code 1962, the US legislature does not state the term 'appropriation'. It defines theft as 'a person is guilty of theft if he unlawfully takes, or exercises unlawful control over, movable property of another with purpose to deprive him thereof'.[5] According to this definition, the appropriation of another person's property occurs when the criminal takes or exercises control over it without the person's consent.

The stated examples and the scholars' literature refer that appropriation may occur only when a physical action happens, such as carrying or taking another person's property away by the accused.

Having sketched this concept of appropriation and the conditions that are required for it, a question arises whether the element of appropriation according to these conditions exists in the crime of identity theft.

It is pertinent to mention here that the author rested his claim on literature drawn from other jurisdictions as well as in other related (to other intangible properties) penal codes such as the trade secret or intellectual property theft laws (that tried to whether trade secret or intellectual property can be subject to theft). One of the obvious reasons is that there is limited literature on the topic particularly in Iraq.

4.1.2.3 Challenges That May be Caused by Applying the Traditional Term of Appropriation to the Misuse of Personal Information

Due to the specific nature of personal information, an obstacle has been created with respect to applying the conditions that are required for the term 'appropriation' that is stated in Iraqi theft offence laws to the crime of identity theft.[6] As a result, a debate has risen about whether the term 'appropriation' causes challenges or difficulties in relation to the application of the term appropriation of theft offence to the crime of identity theft. The debate formed two groups. One of them believes that there are challenges that prevent the application of the term appropriation as used in Iraqi theft offence laws to

[4] Section 3 (1) of the Theft Act 1968 c. 60 (UK)
[5] Section 223.2 (1) of the Model Penal Code 1962 R 12. 9. 5 (US)
[6] A L Christie, 'Should the Law of Theft Extend to Information?' (2005) Vol. 69 Journal of Criminal Law 346-360

identity theft whereas the other believes they are not. Each one of these groups has its evidence. Accordingly, the evidence of each group will be discussed in detail below.

Some scholars[7] believe that the courts may find it difficult to apply the conventional concept of appropriation to the act of unlawful taking of personally sensitive information because this information cannot be 'taken away' or 'carried away' in the traditional physical sense.[8] In addition, certain methods that are used to obtain this information, such as seeing or hearing the information and then memorising it in order to use it to commit other crimes do not fall within the scope of the traditional term 'appropriation'.[9] It is pointed out that personal information cannot be physically taken away or carried away because it is not subject to being physically taken.[10] Nonetheless, it may be subject to physical removal if it is put onto or copied onto movable property. Only in this way can *personal or financial information of people* be taken away or carried away. However, if the defendant transfers or copies information from this tangible property he/she may not be guilty of theft because there is no actual appropriation that refers to depriving the owner of his/her *information*.[11]

Consequently, there is no appropriation if the accused hears or sees another person's

[7] J Clough, 'Data Theft? Cybercrime and the Increasing Criminalization of Access to Data', (2011) Vol. 22 (1-2) Criminal Law Forum 145-170, it was pointed out in his article that confidential information cannot be taken or converted in a manner that resulted in the deprivation the victim, 148 ; Val D Ricks, 'The Conversion of Intangible Property: Bursting the Ancient Trover Bottle with New Wine' (1991) Brigham Young University Law Review 1681-1715, he supported the court's decision and stated that intangible property cannot be subject of conversion unless it is converted as well …. In addition, he stated that the trover action's basic assumed that the property involved must be bound up with tangible property 1713; S P. Green, 'Plagiarism, Norms, and the Limits of Theft Law: Some Observations on the Use of Criminal Sanctions in Enforcing Intellectual Property Rights' (2002) Vol. 54 Hastings Law Journal 167-242, the author stated that if you steal my copy of *Atonement*, there is a physical taking can be proved. But if I make unauthorized copies, there is no physical loss to point to. Someone's use of another person's words or ideas itself deprives another person nothing; R Nimmer, *The Law of Computer Technology* (3rd edn 1997) 12

[8] In the same vein see *Olschewski v. Hudson*, (1910), 87 Cal. App. 282, 262 P. 43

[9] A Tammam, *Crimes Related to Internet Use Comparative Study* (1st edn Dar Al- Arabia Nahda Cairo 2000) 492; *United States v. Bottone*, (1966) 356 F.2d 389, cert denied, 385 U.S 974, 6

[10] M Hosni, *Penal Code Explain Private Section* (Dar Al-Arabia Nahda, Cairo, 1994) 841; U Ramadan, *Penal Code explains Specific Section* (Dar Al-Arabia Nahda 1986) 815

[11] A Al- Huseini, *Important Problems in the Crimes Related to Internet and its International Dimensions* (2nd edn Dar Al- Arabia Nahda without year); Song and Leonetti pointed out that personal information is an intangible form of value, but it cannot be a subject of actual transfer of its possession or control, which resembles the transfer or control of a specific object or power. M Song and C Leonetti, 'The Protection of Digital Information and Prevention of Its Unauthorized Access and Use in Criminal Law' (2011) 13 available at <http://works.bepress.com/carrie_leonetti/14/> viewed on 28 December 2011

information without their consent.[12] However, it has been said that personal information is property and may be obtained or appropriated by any means irrespective of whether the means is physical or non-physical (such as taking away, carrying away, seeing, or hearing).[13] If that is the case, identity theft takes place and a person may be guilty of it if he/she uses another person's information without their consent to obtain illegal purposes.[14]

Moohr[15] pointed out that 'the term of 'taking' is something of a misnomer because intangible property cannot be taken in the strict sense.' It may cause violation to the abstract right of the owner. It is also argued that it is inappropriate to apply the term appropriation that is found in traditional theft offences to the *actus reus* of identity theft because the act of the unlawful obtaining of another person's information carries elements of another crime, such as fraud, not theft.[16]

Due to the lack of courts' decisions in Iraq,[17] the author looks at some decisions from US, and UK and other jurisdictions to support his argument. For instance, he has used a decision that has been decided by the U.S Supreme Court to support the argument that goes against the view, which believes that personal and financial information of individuals may be subject to physical taking. In *Dowling v. United States,*[18] the

---

[12] J Essegair, *Criminal Law and Modern Technology Crimes Arising from the Use of Computer* (1st edn Dar Al- Arabia Nahda 1992) 62; M Shawabkeh, *Computer and Internet Crimes Cyber Crime* (Dar Al-Thaqafa Amman 2004) 154

[13] Ateek, *Internet crimes*, (1st edn Dar Al- Arabia Nahda 2000) 103; A Mahmoud, *Theft of the Stored Information in the Computer*, (3rd edn Dar Al-Arabia Nahda Cairo 2004) 297

[14] Ateek, ibid 103

[15] G S Moohr, 'Federal Criminal Fraud and the Development of Intangible Property Rights in Information' 2000 Vol. 2000 University of Illoins Law Journal 683-739 ; Abdul Moneim claimed that a person's means of identification cannot be subject to physical taking because it is intangible. Tangible things only can be subject to physical taking, interview with Firas Abdul Moneim, assist Professor and Head of law department in School of Law, Baghdad University-School of Law, (Baghdad, 20 February 2013); Al Obeidi and Al Ali claimed that a person's means of identification cannot be subject to physical taking, interview with Ali Al Obeidi and Amer Al Ali, lawyers at Presidency of the Federal Court of Appeal of Baghdad/ Rusafa, (Baghdad, 27 February 2013)

[16] A Steel, 'Problematic and Unnecessary? Issues with the Use of Theft Offence to Protect Intangible Property' (2008) Vol. 30 Sydney Law Review 575-614

[17] The author has not find cases relate to the misuse of the personal information or any other information. The reason behind this lack may be related to the lack of provisions that protect this kind of information or there were no unlawful acts have been committed against it. In addition, most of the courts documents have been destroyed by unscrupulous people after the invasion of Iraq by USA.

[18] *Dowling v United States* 473 US 207 (1985) in this case the US Supreme court discussed the conditions that the National Stolen Property Act of 1934 requires to consider the stolen property has been transferred

Supreme Court pointed out that if the law sets out that a subject of theft should be a physical thing and it should be taken by a physical way. Taking intangible property cannot be subject to theft because it is intangible and cannot be physically taken. However, it has been argued that the term 'appropriation', *which is stated in the current Iraqi theft offence laws,* as a means to commit conventional theft does not take place when other persons take another person's information away, it may be satisfied when the rightful person *loses control* of his information.[19] He loses control of his information because the other persons participate with him in the use of the information and it is no longer confidential.

In summary then, it is submitted that the term 'appropriation' which is used in the current Iraqi theft offence laws makes a challenge in regarding to the application of theft offence laws to identity theft because these laws correspond to movable tangible property. In addition, they require a physical action to obtain another person's property.[20] The term appropriation of theft offences causes a challenge because it occurs when a person's property has been taken, converted, or carried away, whereas the individual's information, as with any intangible property, cannot be taken away, carried away, or converted,[21] as movable property because it is intangible.

Furthermore, some methods that are mentioned early in this thesis and used to commit

---

among states in US. The court stated that recording or copying "phonorecords" and transferring them across a State boundary does not constitute a crime of theft, conversation or fraud under the National Stolen Property Act because this Act requires that the property should be a physical thing and it should be taken by physical means such as taking or converting. For that reason, the accused does not obtain these resources by 'illegal' means; T H Flaming, 'The National Stolen Property Act and Computer Files: A New Form of Property, a New Form of Theft' (1993) The University of Chicago Law School Roundtable 258 available at <http://heinonline.org/HOL/Page?handle=hein.journals/ucroun1993&div=15&g_sent=1&collection=journals> viewed on 29 December 2011

[19] A L Christie, supra, note 6, 352; A Simester and W Brookbanks, *Principles of Criminal Law* (3rd edn Thomsons Brookers Wellington 2007) they mentioned that the ownership and control are considered enough to constitute taking of intangible property 682; Rumbles agreed with the previous view, W Rumbles, 'Theft in the Digital: Can You Steal Virtual Property? (2011) Vol. 17 (2) Canterbury Law Review 370

[20] J T Cross, 'Protecting Confidential Information Under the Criminal Law of Theft and Fraud' (1991) Vol. 11 (2) Oxford Journal of Legal Studies 264-272

[21] C J Dickson, E Beat, L M Wilson and JJ Le Dain, Indexed as *R. v. Stewart*, File No. : 17827, 26 May [1988] 1 S.C.R. 963, 3, 963 available at <http://scc.lexum.org/en/1988/1988scr1-1097/1988scr1-1097.pdf> accessed on 10 December 2011

identity theft (such as phishing, shoulder spoofing, or spamming) are not acts of 'taking away' or 'carrying away'. There is also a difference between taking tangible property and intangible property. If tangible property, for instance, has been taken away the owner may lose possession and effectively other rights that are attached to the property. In contrast with appropriation of tangible property, if personal information has been appropriated the owner loses nothing and he still has the ability to use the information. Accordingly, personal information cannot be the subject of traditional appropriation. Moreover, in the case of tangible property, if the perpetrator takes or carries the movable thing away, he can return it to the victim or dispose of it. However, with intangible property, it is impossible for the perpetrator to return or dispose of the information if he/she memorises it. Even if the perpetrator is prohibited from using this information, he/she still possesses what he/she heard and memorised.

The argument whether a person's means of identification can be subject to physical taking remains contestable among scholars and professionals, however, if one accepts the notion that personal information can be a subject of physical taking, another issue may be raised is whether personal information can be labelled as property?

4.2 Difficulties That May Be Caused by Labelling Personal Information as Property

A general idea should be given about the term 'property' before starting to scrutinise whether this term, which is an element of traditional theft offence can be established in personal information.

4.2.1 Definition of Property as an Element of Traditional Theft Offences

The Iraqi legislation does not define the term 'property', but it mentions in section 439 of Iraqi theft offence laws that a person may be guilty of theft if he appropriates 'movable property or electric power', whereas the UK and the US jurisdictions that are chosen as a reference in this study define it. The UK legislature in section 4(1) of 1968 Theft Act defines the term 'property' as money and all other property, real or personal including things in action and other intangible property. The US legislature in section 223 of the Model Penal Code also defines the term 'property' as:

> 'anything of value, including real estate, tangible and intangible, personal property, contract rights, choses-in-action, and other interests in or claims to

> wealth, admission or transportation tickets, captured or domestic animals, food and drink, electric or other powers.[22]

Iraqi jurisprudence, therefore defines the term property as everything that has a physical entity, a value and that the law considers a subject of transaction, such as money, goods, food, and chattel among other things,[23] the term 'property' stated in the current Iraqi theft offence laws seems to deal with movable property only.[24] This property requires some conditions to be subject to theft, such as it should have value, be subject to possession or it can be subject to control by a person or people. Therefore, the issue that arises is whether personal information encompasses the same elements of tangible property and maybe protected by Iraqi traditional theft offence laws.

4.2.2 Possible Challenges to Labelling Identify Personal Information as Property

A debate has risen among scholars and professionals related to whether personal information is property according to the definition of property stated in Iraqi theft offence laws. The debate forms two groups.

According to the first group's opinion, it is said that the individual's information cannot be subject to theft[25] because personal information by its very specific nature is incapable of exclusive possession.[26] Following the notion of the definition of theft in Iraqi legislation, the concept of property in this legislation appears to require physical or tangible property.[27] Consequently, this view restricts the theft offence to tangible property. It is also stated that the crime of theft is a complex crime and the meaning of

---

[22] Section 223.0.6 of the US Model Penal Code (2006)

[23] U Ramadan, supra, note 10, 434

[24] Section 439 of the Iraqi Penal Code 1969

[25] A Reed and B Fitzpatrick, *Criminal Law* (4th edn Sweet and Maxwell Limited 2009), 458; R Heaton, supra, note 3, 277-292; D Ormerod, *Smith and Hogan*, *Criminal Law* (12th edn Oxford University Press 2009) 756; A Coleman, 'Trade Secrets and the Criminal Law in Canada' (1988) Vol. 10 (1) Eur. Intell. Prop. Rev. 15-18; R.G. Hammond, 'The Misappropriation of Commercial Information in the Computer Age' (1986) Vol. 64 Canadian Bar Review 349- 52; R.G. Hammond, 'Theft of Information' (1984) 100 L.Q. Rev. 252, 256-60; C Reed and J Angel, *Computer Law: The Law and Regulation of Information Technology* (6th edn Oxford University Press New York 2007)

[26] J Cross, 'Trade Secrets, Confidential Information, and the Criminal Law' (1991) Vol. 36 McGill L.J. 534; *Dowling v. United States*, 473 U.S. 207 (9th Cir. 1985); *United States v. Ochs* 842 F.2d 515, 521 (1st Cir., 1988); *United States v. Brown*, 925 F.2d 1301 (10th Cir., 1991); *McNally v. United States*, 483 U.S. 350 (6th Cir. 1987)

[27] L Macpherson, 'Theft of Information' (1994) Vol. 63 (3) Scottish Law Gazette 93; *United States v. Gimbel* 830 F.2d 626, 627 (7th Cir. 1987)

the elements is unclear.[28]

Due to the lack of Iraqi courts' decisions,[29] the author sometimes cites or uses courts' decisions from either the UK, US courts or courts of other jurisdictions to support his argument. Therefore, the author supported the above scholars' view by a decision that was held by one of the British courts in *Oxford v Moss*.[30] As it was shown from the previous definition of theft stated in the UK legislation, the UK legislator expanded the term 'property' to encompass even intangible property; however, the British court in this case did not brand confidential information as property. The facts in this case were an engineering student got hold of the upcoming exam paper. He read and copied the information from the exam paper and then returned the original. The court held that the information that was taken was not property. The court reasoned that this private information did not fall within the scope of the definition of property for the purposes of theft. This decision was subsequently adopted by Canadian Courts, with respect to stealing a list of employees' names that was held by a hotel.

For instance, in *R .v. Stewart,*[31] the Canadian Supreme Court, (1988) held that personal confidential information is not property. The fact in this case is a perpetrator was hired by another person to obtain the personal information of the hotel employees. The information was kept secret because the management of the hotel had previously refused to disclose it. He was arrested and accused of counselling others to commit theft and fraud. At the trial the perpetrator was acquitted. The court pointed out in its decision that the confidential information to be a subject of theft it must be capable of being property and that personal confidential information is not property. However, the majority in the Court of Appeal convicted the perpetrator of counselling others to commit theft. They believed that an individual or individuals' information might constitute a stolen object.[32]

---

[28] A Steel, supra, note 16, 575

[29] The author could not find decisions from Iraqi courts because cases have not come before these courts. In Iraq, there are no provisions that deal with the misuse of information as intangible property. Most of the rules that are found in the existing Penal Code 1969 deal with the misuse of tangible property. Even if it assumed that there were some cases handled by Iraqi courts they might disappear because unscrupulous persons destroyed courts documents during the US invasion of Iraq.

[30] *Oxford v Moss* [1979] 68 Cr App Rep 183

[31] *R. v. Stewart*, [1988] [1988] 1 SCR 963

[32] *R. v. Stewart*, [1983] 42 O.R. (2d) 225; 149 D. L. R (3d) 583

In the Supreme Court, the accused was acquitted. The Supreme Court held that personal information could not be property for the purposes of theft.[33] It reasoned that property might be a stolen object if it is capable of being taken in a way that causes the owner to be deprived of it.[34] However, the list of employees' names failed to satisfy any of the elements of theft that are stated in the Criminal Penal Code of Canada because it was not property, and it was not something that could be taken in a way that may result in deprivation to the owner.[35] The Supreme Court's decision supported a decision was held by the Alberta Court in *R. v. Offaly*.[36] In this case, Ontario Court of Appeal held that personal confidential information is property and it may be a subject of theft. However, the Albetra Court has objected to this decision and held that confidential information cannot be subject to theft.

The above decisions encourage the study to conclude that personal information is not property according to the term of Iraqi theft offence laws because these laws confined

[33] *R. v. Stewart*, supra, note 31

[34] ibid

[35] *R. v. Stewart*, [1988], ibid. Section 322 of Canadian Criminal Code 1970 states that: (1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything, whether animate or inanimate, with intent (*a*) to deprive, temporarily or absolutely, the owner of it, or a person who has a special property or interest in it, of the thing or of his property or interest in it; (*b*) to pledge it or deposit it as security; (*c*) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform; or (*d*) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.
Time when theft completed: (2) A person commits theft when, with intent to steal anything, he moves it or causes it to move or to be moved, or begins to cause it to become movable.
Secrecy: (3) A taking or conversion of anything may be fraudulent notwithstanding that it is affected without secrecy or attempt at concealment.
Purpose of taking: (4) For the purposes of this Act, the question whether anything that is converted is taken for the purpose of conversion, or whether it is, at the time it is converted, in the lawful possession of the person who converts it is not material.
Wild living creature: (5) For the purposes of this section, a person who has a wild living creature in captivity shall be deemed to have a special property or interest in it while it is in captivity and after it has escaped from captivity.

[36] *R. v. Offley* [1986] 28 C.C.C. (3d) 1 in this case, the defendant operated a business which achieved security checks on job applicants for employers. Defendant has been required to pay a member of the Edmonton City Police Department two dollars per name for running the name through the police data bank. The defendant was arrested, charged, and convicted of the crime of counselling theft of information stored in the police database. In the Court of Appeal, the conviction was reversed. In his comments the Justice Belzil pointed out that the defendant had no in any way deprived the Edmonton Police of property because the information at all times was in their possession, and they had retained full use of it. He added that it made no sense to talk of refunding something to the owner in a condition different from that when it was 'taken' because there had never been a taking in the first place.

the term 'property' with movable property only. It could be said that Iraqi theft offence laws have been enacted to protect movable property that consists of the elements: possession, ownership, or control. However, these elements do not easily lend themselves to be applied to theft of personal or financial information of another person.[37] This can clearly be shown in UK courts decisions. Although the UK legislature extended the scope of the term 'property' to encompass some intangible property, the UK court, however, decided that confidential information did not fall within the scope of the definition of property and it cannot be subject to theft. [38]

Biograd[39] also mentioned that personal information is not property, particularly; that appears on a screen and it cannot be subject to theft. However, it may be subject to theft if it is recorded or copied onto a computer disk, magnetic tape or any other tangible thing,[40] it should be considered property.[41] In addition, it is argued that personal information is an immaterial thing and cannot be property because material things only may be property. [42] Furthermore, Ghannam[43] points out that the crimes of theft are committed against possessions and possessions can only be in physical things. As a result, personal information, which has only an incorporeal entity, cannot be subject to theft because it cannot be object to possession.

However, it is argued that personal information is property because it has a physical entity by which it can be viewed via a physical material, such as a computer screen or *a credit or debit card*. It may therefore belong to the person who possesses or creates it to

[37] J T Cross, supra, note 26, 264-272
[38] *Oxford v Moss*, 1979, supra
[39] M Biograd, *Analysis Study of Theft and Appropriation, a Research Presented to the Six Conference of Egypt Group of Criminal Law*, (Cairo 1993) 372
[40] M Hosni, supra, note 10, 815; A Tammam, supra, note 9, 463
[41] In case *Boardman v. Phipps*, the court stated that information is not property in any normal sense, but if it is taken away in breach of some confidential relationship equity will restrain its transmission to another. (1967) 2 A.C. 46
[42] Ateek, supra, note 13, 297; A Mahmoud, supra, note 13, 152; U Al-Huseini, supra, note 11, 102-119; H Rustom, *Penal Code and the Dangerous of Information Technology* (Modern Tools Library without published year) 29
[43] K Ghannam, *Traditional Rules in Penal Code are Insufficient to Combat Computer Crimes*, (Emirates University 2000) 10

use for their own benefit. [44] In addition, it may be sold, rented, be the subject of trust, or it may even be bequeathed. According to above considerations, it appears that Iraqi theft offence laws could protect personal and financial information of people.

It seems from the debate above that those who believe that personal information is not property depend on the elements of property to establish personal information as property. They state that property consists of three elements: possession, ownership, and control over the thing, however, these elements do not exist in personal information. Consequently, personal information is not property and it cannot be a subject of theft.

However, notions, the British Court, and Canadian courts' opinions that supported them have been criticised by the second camp. It is argued that those notions and both the British and Canadian courts failed to justify that personal information is property. Personal information may be subject to theft[45], and judgments like this can have anomalous consequences.[46] For instance, if a person seizes a paper or a file containing confidential information, regardless of its value, he is guilty of theft, whereas a person who only memorises or copies the information that this paper or file contains, is not guilty of theft.[47]

With respect to the discussion regarding whether virtual goods are property, it has been said that these goods are property because they comprise most characteristics of property (such as possession, using, enjoyment, transferring, and excluding others from

[44] H Kashkoush, *Computer Crimes in the comparative legislation* (Dar Al-Arabia Nahda Cairo 1992) 53; M Shawabkeh, supra, note 12, 141; A Al-Qahwaji, *Criminal Protection of Computer Programs* (1992) Journal of Collage of Rights for the Economic and Law Research); A Mahmoud, supra, note 13, 290

[45] *United States v. Seidliz*, 589 F.2d 152 (4th Cir. 1978); *United States v. Cherif* 943 F.2d 692 (7th Cir. 1991); *United States v. Czubinski* 106 F.3d 1069, 1074 (1st Cir. 1997)

[46] M Jefferson, *Criminal Law* (10th edn Pearson Education Limited London 2011) 603

[47] A S Weinrib, 'Information and Property' (1988) Vol. 38 (2) University of Toronto Law Journal 117-150; Davies criticised section 4(1) of Theft Act 1968 and stated '……[t]his, of course, leads to the ridiculous situation where if a large corporation uses a patent belonging to another making several million pounds in profit, it is not guilty of an offence, but if the information is stored on a floppy computer disk which takes to get the information and which may only be worth a few pence, it is guilty of an offence of theft.' There is actually no reason why appropriation of patent is not considered theft. '. …a patent is personal property capable of being sold, licensed and otherwise dealt with.' C R Davies, 'Protection of Intellectual Property –A Myth? A Consideration of Current Criminal Protection and Law Commission Proposals' (2004) Vol. 68 Journal of Criminal Law 398-410; as well, Christie stated that the theft of boardroom table is punished far more severely than the theft of the boardroom table secret. See A L Christie, supra, note 6, 349

using it).[48] This may make it as property that is capable of being a stolen subject. Fairfield[49] when he discusses whether virtual goods as property agrees with this view that these goods are property and expands the general definition of theft to include it. In addition, he states that these goods have three characteristics resembling real property, such as it is being used to obtain goods, persistence and interconnectivity.

Moreover, it is argued that personal information, which has been appropriated from the computer or the internet, constitutes a new property and a new kind of crime of theft. Accordingly, its physical possession is an inevitable fact.[50] However, a negative approach has been taken against the previous opinions. It has been stated in this negative approach that intangible materials (a person's information) cannot be deemed to be property because it is unformed and shapeless.[51] It has been mentioned that personal information does not resemble movable property and therefore it should not be subject to criminal protection. In the same vein, Carrier and Lastowka[52] argued that personal information could not be the subject of theft because this information lacks the fundamental characteristics of the concept of property in the civil law and does not have property rationales or effective boundaries.

Turn to the argument for personal information as property; there is another tendency that believes that personal information as physical property consists of a package of rights limited to the owner. These rights confer on the owner a right to prevent the illegal use and disclosure of that information[53] without their consent. This, therefore, may be enough to make the information subject to theft. It is said that there is no difference between intangible and tangible property when applying *the current Iraqi* provisions of theft to a person who illegally uses another person's information without

[48] A V Arias, 'Life, Liberty, and the Pursuit of Swords and Armor: Regulating the Theft of Virtual Goods,' (2008), Vo.57, Emory Law Journal 1301-1346.

[49] Joshua A.T. Fairfield, 'Virtual Property' (2005) Vol. 85 Boston University Law Review 1047-1102

[50] Flaming, supra, note 18, 290-91; *United States v. Carpenter*, 484 U.S. 19, 108 S.ct. 316, 98 (1987)

[51] G S Moohr, supra, note 16, 693; *United States v Brown*, 925 F2d 1301, 1308-09 (10th Cir. 1991), in this case the Court of Appeals, Holloway, Chief judge, held that computer program was intangible intellectual property, which could not be a subject of theft, converted or taken within the meaning of National Stolen Property Act because it could not constitute goods, wares, merchandise, securities or monies, which are considered subjects of theft.

[52] A Michael Carrier and G Lastowka, 'Against Cyberproperty' (2007) Vol. 22 Berkeley Technology Law Journal 1485-1520; see also *McNally v United States* 483, U.S. 350, (1987)

[53] A S Weinrib, supra, note 47, 127; Section 322 of the Canadian Criminal Code 1970

his/her consent because it is not necessary that theft can only be committed against physical property.[54] In addition, some scholars[55] pointed out that property is a term that refers to 'all things whether tangible or intangible' belonging to individuals, companies or governments, such as money, things in action, cheques and land. They pointed out that theft offences might be applied, for instance, to a person who takes or carries away an item that has a value when it is in the possession of another person without that person's consent.

The debate is continuing among scholars and professionals with regard as to whether personal information is property. As a result of this debate, Al-Showa[56] argues that even if personal information is an intangible material and the term property corresponds only to tangible property, it still has an economic value and sometimes utilised as a means to inflict damage upon another person. Therefore, it should be protected by *existing Iraqi theft offence laws*. In addition, some scholars[57] state that criminal theft law does not only protect properties that human beings possess, however, it can protect all properties or things which have value and fall under the control of human beings, such as electricity and any other power. Consequently, a person's information can be subject to theft because it falls under the control of a human being. However, one might argue that not everything that has value can be protected by the theft statute. For instance, there are many things that have value, such as a human being or people's sense of safety, but are not governed by the theft statute, because they cannot be classified as a species of property.[58]

Frank,[59] in his comments in *Kremen v. Cohen*, states that theft offence laws were enacted to protect only properties that are subjects to buying or selling and personal

[54]A Mahmoud, supra, note 13, 304; A V Arias, supra, note 48

[55] A Reed and B Fitzpatrick, supra, note 25, 457; M Molan, D Bloy and D Lanser, *Modern Criminal Law* (2003) 257

[56] M Al-Shawa, The *Information Revolution and its Implications to the Penal Code*, (2nd edn Dar Al-Arabia Nahda, 1998) 171, M Hiti, 'Difficulties That May Obstruct the Application of Iraqi Theft Offence Laws to Crimes against Computer Programs' (2004) Journal of Sharia and law, United Arab Emirates

[57] InsuWhang, 'The Property Concept in Criminal Law' Dissertation of Sungkyunkwan University (2006) 38; Hyunggak Lee, Property in Criminal Law, Dissertation of Yonsei University (1988)

[58] S P. Green, supra, note 7, 217

[59] C W Franks, 'Comment Analyzing the Urge to Merge: Conversion of Intangible Property and the Merger Doctrine in the Wake of *Kremen v Cohen*' (2005-2006) Vo. 42 (489) Houston Law Review 490-527

information cannot be sold or bought because it is not a subject of buying or selling. However, he states that *personal information* can be protected by the *current Iraqi theft laws* because criminal law precludes appropriation of "anything of value" and this preclusion of appropriation comprises both tangible and intangible property. Green[60] agreed with a part of Frank's opinion and differed with another part of it. He agreed with the part of the view, which argued that the theft offence statutes were enacted to protect the thing that could only be sold or bought, but he disagreed with the part that argued the manner that can be used to protect personal information. He pointed out that *personal or financial information of individuals* could be protected, not as a kind of property or anything of value, but through determining the kinds of rights or interests of theft that the law intended to protect them.

To obtain more evidence that may support and help the study in its analysis to appreciate whether personal and financial information of people is property and then can be govern by theft offence laws in Iraq another decision from the Canadian Supreme Court will discussed.

In its decision that related to *C Schweppes Inc v FBI foods Ltd,*[61] the Canadian Supreme Court stated that even if the individuals' information is not property it is confidential, and a breach of confidence of information might constitute sufficient grounds to punish the perpetrator. However, the same Court in *R. v. Stewart*[62] had previously stated that the confidentiality is divorced from the information itself; bare confidentiality cannot be a form of property. Therefore, there is not sufficient ground with a breach of confidence to punish the accused of a crime, such as theft. The reason behind these two different decisions is that the court in first decision sought, through depending on civil rules, to remedy the relationship between parties, whereas in the second decision it sought to punish the person who committed the illegal act against society. As will be seen in the next section, the concept of property in civil law differs from the concept of property in criminal law.

[60] S P. Green, supra, note 7, 216
[61] *C Schweppes Inc v. FBI foods Ltd* [1999] 1 SCR 142
[62] [1988] 1 SCR 963

Mahmoud[63] in his argument to establish the property in intangible things (personal information) and find a base to protect it from the illegal use equates it to electricity power and phone line. This is true even if the information is intangible things and it cannot be appropriated by a physical means. However, it resembles electricity and telephone line, both are not movable materials, but some legislation, most judges and jurisprudence consider electricity and telephone line to be a subject of theft. Consequently, personal information, as with electricity and telephone lines, could be a subject of theft.[64] This view has been criticised because one cannot compare the unlawful use of information with the theft of electricity because there is a difference between the information and the electricity and telephone line. The information is not power and therefore it cannot be a subject of theft. In addition, even with the theft of electricity and the telephone line, there is no theft of the electric pulses or phone calls. The theft is committed against the use of the electricity or the telephone lines, not the conversation between people.[65]

In a bid to justify personal information as property, it is argued that the judge can apply the term of metaphor.[66] This means that the judge can use the words as synonyms, such as 'space', 'place', or property to allow the judge to think of the personal information as similar to physical property. As a result of this view, the Courts can consider intangible things to be tangible properties in order to protect the individual's or individuals' information[67] from the unlawful misuse. Furthermore, it is stated that personal information as tangible property should be an object, which is capable of being a stolen subject not just for criminal theft provisions, but also according to the modern civil

[63] A Mahmoud, supra, note, 13, 296; Abdul Moneim claimed that people's means of identification is not property. It has no value. It cannot be subject to sell or rent. It is intangible, interview with Dr. assistant Professor Firas Abdul Moneim, the Head of law department at University School of Law (Baghdad, 20 February 2013); Al Fatlawi claimed that a person's means of identification is a right that is considered closely to the person, but it is not property. It belongs to him, but it is not property, interviewed with Dr. assistant Professor Salah Al Fatlawi, a lecturer and Deputy Head of School of Law of Baghdad University (Baghdad, 16 February 2013)

[64] A Mahmoud, supra, note, 13, 447

[65] P Samuelson, 'Is Information Property?' (1991) Vol. 34 (3) Communication of the ACM 15-18

[66] D McGowan, 'The Trespass Trouble and The Metaphor Muddle' (2004) Legal Studies Research Paper Series Research Paper No. 04.5, 2 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=521982> viewed on 20 November 2011

[67] J D Lipton, 'Mixed Metaphor in Cyberspace: Property in Information and Information Systems' (2003) Vol. 35 (1) Loyola University of Chicago Law Journal 235-274; D McGowan, 'The Trespass Trouble and the Metaphor Muddle' (2005) Vol. 1 (200) Journal of Law, Economics & Policy 109-146

notion of property. If this were accepted, it would protect wider interests than just land and tangible property.[68]

It has also been stated that with the absence of a specific statute that determines whether personal information is property, the judge should rely on the traditional statute of property offences to protect an individual or individuals' information from the unlawful misuse. [69]

In sum, the debate for establishing property in personal information has been presented by two approaches. The first approach expressly states that personal information is property and it can be a subject of theft, whereas the second approach does not expressly state that personal information is property. It tries to find a base to label personal information as property. In light to the debate above, it could be argued as some scholars pointed out that to protect personal information, *particularly a person's means of identification* from the misuse or appropriation, new legislation should be enacted to determine and clarify precisely when information should be treated as property, and when not. There is no world in which all information belongs to its discoverer. Thus, a new theory about when information should be labelled as property and when not, is required.[70]

4.2.3 A Bid to Transfer the Concept of Information as Property from Civil Law to Criminal Law

As stated previously, there is limited literature and courts decisions that deal with the act of the unlawful obtaining of another person's means of identification. In addition, as it appeared from the decisions that were stated previously the US and UK courts face the same difficulties that the Iraqi courts may face when they apply the term of property to personal or financial information. As a result, the US and UK courts tried to discuss the concept of property in civil law in a bid to justify that personal information is property, and then transfer the result to theft offence laws. In order to appreciate whether these efforts can be adequate to assist the Iraqi judges to transfer the concept of

[68] A S Weinrib, supra, note 47, 119

[69] S W Branner, 'Is There Such a Thing as "Virtual Crime"?' (2001) Vol.4 (1) California Criminal Law Review 1-72

[70] P Samuelson, supra, note 65

property from civil law to criminal law these attempts will be examined below.

The US courts adopted two approaches: (1) misappropriation or property theory and (2) an equity or obligation approach. According to the misappropriation or property theory, the US courts held that a person possesses his confidential information and no one can use this information to obtain benefit for himself or for another without a right over it.[71] As Hammond mentioned the US courts held that a person could not reap where he has not sown.[72] As a result, the courts held that the personal information of another person should not be disclosed to others without his consent.[73] This theory has been criticised because it represents the court's view.[74] It is argued that the theory does not give a reasonable basis to justify personal information as property. Consequently, the US courts have tried to justify personal information as property in an equity or obligation approach.

In the equity or obligation approach, the accused connects with the owner of the information by a contract, which is called a fiduciary contract.[75] If the accused exploits his position and discloses or uses the confidential information without consent, he may be liable for the information disclosure.[76] He may be held accountable for civil and/or criminal liability.[77] Hammond[78] stated that the US courts have held that the prospective

[71] *International News Service v. Associated Press*, 248 U.S. 215 (1918)

[72] R G Hammond, 'Is Breach of Confidence Properly Analysed in Fiduciary Terms?' (1979) Vol. 25 McGill Law Journal 244-253

[73] *Chiarella v. United States*, 445 U.S. 222 (1980), 'in sum, the evidence shows beyond all doubt that Chiarella, working literally in the shadows of the warning signs in the printshop, misappropriated -- stole, to put it bluntly -- valuable non-public information entrusted to him in the utmost confidence. He then exploited his ill-gotten informational advantage by purchasing securities in the market. In my view, such conduct plainly violates § 10(b) and Rule 10b-5. Accordingly, I would affirm the judgment of the Court of Appeals.'

[74] R G Hammond, Is Breach of Confidence Properly Analysed in Fiduciary Terms, supra, note 72, 244-253

[75] J Wilson, 'Confidential Information-Recurrent Problem and Recent Developments' (2009) 1 available at <http://www.11kbw.com/articles/docs/JulianWilsonConfidential_Information.pdf> viewed on 30 December 2011

[76] J E Stuckey, 'The Equitable Action for Breach of Confidence: Is Information Ever Property?' (1980-1982) Vol. 9 Sydney Law Review 402-432

[77] R M Halligan, 'Duty to Identify, Protect Trade Secrets Has Risen' (2005) The National Law Journal, the Weekly Newspaper for Local Profession, available at <http://www.thetso.com/Info/National%20Law%20Journal%20Article.pdf> viewed on 30 December 2011

[78] R G Hammond, 'Quantum Physic, Econometric Models and Property Right to Information' (1981) Vol. 27 McGill Law Journal 47-72

business opportunity that has been taken by this fiduciary contract belongs to the client. The courts also stated that the confidential information is treated as economic goods regardless of whether it is property or something, which could rationally have been expected to mature into a property interest.[79]

Whereas the UK courts tried to find basis of property in personal information through a breach of confidence and breach of a fiduciary contract approaches. A breach of confidence means there are some express or implicit obligations that may be found between the owner of information and the plaintiff. If the plaintiff discloses the confidential information without consent, he may be guilty of a breach of confidence.[80]

A fiduciary contract means a contract between the owner of information and another person who reserves or deals with this information, such as agencies, solicitors or any other person who can view or reach the confidential information.[81] According to the approach of a fiduciary contract, the owner of the information has a property right in the information. This right requires that confidential information must be secret. Therefore, the UK courts believe that a property right may be created by obligation that arises from an express or implied consensual commitment or an express fiduciary commitment[82] pertaining to the disclosure of the information and the owner.[83]

A main requirement of the fiduciary contract is confidential information must be given to the accused during this contract. Accordingly, the judge Megarry in *Coco v Clark*[84] stated that if the accused gets the confidential information outside the fiduciary contract he might not be guilty of a breach of fiduciary contract.

---

[79] *Robinson v. Brier* 194, A. 2d 204, (Pa. 1963); *Franco v. J.D. Street & Co*. 360 S.W. 2d 597(Mo. 1962); *Gaynor v. Buckley* 203 F. Supp. 620 (Dist. Court D. Oregon. 1962); *Irving Trust Co. v. Deutsch* 73 F.2d 121(2nd Cir. 1934)

[80] *Seager v Copydex Ltd* [1967] 1 WLR 923 in this case, the plaintiff during his negotiation with the claimant got information about new carpet grip features. After the negotiation came to nothing some latter time, the defendant found out a grip themselves, which is considered an integral part of the idea of the claimant's modified a grip. The Court of Appeal pointed out that the defendant's act considered a breach of confidence that is given to him by claimant.

[81] CD Freedman, 'The Extension of the Criminal Law to Protecting Confidential Commercial Information: Comments on the Issues and the Cyber-Context' 2005, 4 available at <http://www.bileta.ac.uk/99papers/freedman.html> viewed on 27 June 2011

[82] R G Hammond, Quantum Physic, Econometric Models and Property Right to Information, supra, note 78 , 57

[83] CD Freedman, supra, note 81

[84] *Coco v Clark* [1969] RPC 41

Having explored the two approaches of the US and UK courts to adopt the concept of property in civil law and to transfer it to criminal law, the author suggests that transferring the concept of property from civil law to criminal law is unworkable. Fundamental differences between civil law and criminal law may prevent the use of the concept of property in civil law as a means to assist the Iraqi criminal judge to label personal information as property. The civil law is concerned with making a balance between the interests of the parties who are involved in dispute whereas criminal law is concerned with wrongs that are committed against society.[85]

In addition, there are legal outcomes that can result if the information is considered property in civil law, which differ from those that may result under criminal law.[86] For instance, the concept of property in the criminal law is broader than the concept of property in the civil law. Furthermore, criminal law may punish the person who takes or carries goods away, such as cocaine that are not considered property in the civil law. What is more, if the information is considered property in the civil law, this does not mean that it is property in the criminal law.[87] More so, personal information as a form of property may be plainly rejected because it cannot be taken or converted in a physical action.

After the argument for and against information as property, a question may arise here: what standards are used to describe personal information 'a person's means of identification' as property? Do these standards the same standards that are used to prove property in a physical material, such as possession, ownership, and control over things, which means the owner can use his personal information in the same way that by which he uses his physical property? In other words, can the owner sell, destroy, give his personal information to another person, or abandon it as with corporeal property, or can he possess identifiers that are considered abandoned or are not owned by others? Can a person buy another person's identifiers? Consequently, persons' identifiers can be inherited to their families after their death and members of their families can use them after the persons' death.

[85] J Clough, supra, note 7, 154-170
[86] J Cross, supra, - note 19, 256
[87] A L Christie, supra, note 6, 351

In effect, as will be shown in the next chapter the legislation and courts do not apply these standards to certain cases. For instance, most world legislations consider a person who does not use his real name, but uses another name, such as a false name, which may not be owned by anyone to gain benefit guilty of fraud. Whereas they do not consider him guilty of an offence when he uses an abandoned physical property or it is not owned by another person, such as wild creatures. On this base, it could be argued that individuals' identifiers are unique things attached to them and they are used to distinguish individuals from each other. Therefore, people's identifiers might not be *actual property* because they may not meet the real elements of *property*.

To summarise the argument for and against personal information as property, it could be argued that this argument is unhelpful alone to resolve the fundamental question that is whether personal information is property and consequently be a subject of theft. Each one of the two groups provides evidence that can be used to support the argument for or against personal information being property. The evidence of the argument against personal information is not property is stronger than the evidence of the argument for personal information as property. It has been supported by three precedents. One of them was adopted by the British court and the others were adopted the Canadian courts.

It appears from the argument for and against personal and financial information as property that this information might not be property according to section 439 of the Iraqi theft offence laws because this section deals with the movable property as a subject of theft and some intangible properties only. The UK and US legislation also have failed to protect personal information against the illegal misuse by other people and they still seem to address tangible property only.

It is submitted that an individual or individuals' information cannot be property because it is incapable of being taken and cannot be replaced by another thing. In addition, it cannot physically be transferred from one person to another, whilst tangible property that may be a stolen object should be capable of being taken or converted in a method that may deprive the owner of their property.[88] Furthermore, if the personal information is considered property, it may be sold, bought, or rented to others, and that might be unimagined with personal information. What is more, even though an individual's

[88] C J Dickson, et al, supra, note 20, 3; *R. v. Offley* (1986), 28, C.C.C. (3d) 1

information is very important to him, it is a range of ephemeral symbols, and it may be changed repeatedly. Moreover, the legislation sometimes and the Courts in general require some conditions to consider a thing as property, such as it should be tangible[89] and has value, while individuals' means of identification are intangible things and have no value,[90] thus, they are not property.[91] Hence, it is difficult to imagine[92] that an individuals' information may be factual property.

The above view can be supported by many facts, for instance, some American statutes, such as the American Intellectual Property Law, Copyright Law, Trade Secret Law, as well as United States Supreme Court have, until recently, not considered confidential information as property.[93] In addition, when the British courts applied the Theft Act of 1968 to the accused who took confidential information without consent they did not consider the act of the unlawful taking of this information as a crime. For instance, as mentioned in the *Oxford* case, the court decided that the person who took the forthcoming exam paper and copied it was not guilty of theft because the exam information, which he took was not property under section 4 (1) of the Theft Act 1968.[94]

Furthermore, the Civil Courts have protected individuals' information not as property, but rather because the protection of this information (as mentioned above), stems from a breach of a confidence obligation or a fiduciary relationship.[95]

On the other hand, if the information is considered property, it may cause undesirable consequences, particularly, if it is obtained, for instance, through the commission of a crime; how can the accused return the information that he/she has stolen? It is very

[89] A Steel, supra, note 16, 584
[90] ibid, 575
[91] *The Case of Swans* (1572–1616) 7 Co Rep 15b; 77 ER 435; *Blades v Higgs* (1865) 11 HLC 621, 11 ER 1474, 628, in this case it was held that "animals *ferae naturae* are divided into two classes; first, such as are vermin, or unprofitable to man; secondly, such as are known as game, and such as are profitable to man. In the first class no one has any property; in the second there is a qualified property"; Section 223.0.6 of the US Model Penal Code.
[92] A Steel, supra, note 16, 575
[93] P Samuelson, 'Information as Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?' (1989) Vol. 38 (2) Catholic University Law Review 365- 400
[94] *Oxford v. Moss*, [1979], in this case was an undergraduate unlawfully obtained an examination paper and returned the original paper after he had read its contents.
[95] C J Dickson, et al, supra, note 20, 16

difficult to return personal information that has been stolen, especially when the information is kept in a person's memory, because he/she is incapable of relinquishing it.[96] An issue that can be considered and may be more of an important reason to defeat the view that personal information is a property. The issue is if a person's dead body cannot be considered property, and it cannot be a stolen object,[97] how then can his/her name, address or his/her date of birth be property subjected to theft?

It might be said that the below circumstances are considered strong rational reasons to protect personal and financial information of people from being misused by unscrupulous persons. The numerous abuses of individuals' information by persons and then use it to commit unlawful activities, such as fraud, may include opening a new account in the victim's name, or taking over his/her existing account by using his/her PIN or social security number, and carrying out terrorist operations under his/her name. Governments also store their information and their citizens' information on computers connected to the Internet. Therefore, that information is available on the internet, and anyone can easily obtain information about any person, financial institution, government, or even members of the government. Moreover, the internet now connects the entire world, and perpetrators can use it to obtain information to accomplish their illegitimate purposes. Those perpetrators use sophisticated methods (such as phishing, spyware programs, viruses, Trojan horses and worms) to obtain people's information, in which it is difficult for people to be aware that they fall victim of identity theft. What is more, perpetrators have the ability to conceal their illegal activities and do not leave any evidence of them.

However, a person's personal and financial information cannot be protected as *actual property* because it does not meet the elements of this property. It could be said that to prevent unscrupulous persons from the unlawful use of other individuals' information to gain illegal ends for them or for others and to enhance individuals' confidence in financial institutions, personal and financial information should be determined as a specific type of property by either a decision or specific legislation.[98] This specific type of property that personal information can be labelled with is *fictional property*. It can be

[96] C J Dickson, et al, supra, note 20, 17
[97] R Heaton, supra, note 3, 292
[98] C D Freedman, supra, note 81, 4

appropriated by any means irrespective of whether it is a physical or non-physical means. Accordingly, the Iraqi legislature is requested to amend existing theft offence laws or enact a specific Act that considers personal information as *fictional property*.

4.3 Belonging to Another

It is important to give an idea about the element of belonging to another before examining whether it causes difficulties to apply theft offences laws to identity theft.

4.3.1 General Concept of Belonging to Another

The Iraqi legislature in section 439 of theft offence laws states that a person is guilty of theft if he appropriates movable property, which does not belong to him.[99] The US legislature describes the term 'belonging to another' as 'property of another' and defines it as 'includes property in which any person other than the actor has an interest which the actor is not privileged to infringe, regardless of the fact the actor also has an interest in the property.'[100] Whereas when the UK legislature defined the term 'belonging to another', it stated that property shall be regarded as belonging to any person who has possession, ownership, or control of it.[101]

It appears that the definition in the UK legislation more unmistakable than the definition in the Iraqi and US legislation. According to the UK legislation, the property belongs to a person if he has possession, ownership, or control over it. The majority of the Iraqi jurisprudence agreed with the UK legislature that the term of belonging to another requires the person has possession, ownership and control over the property. However, this is not essential because a person sometimes has control of the property, even though it does not belong to him/her. For example, the person who eats in the restaurant has control of the cutlery, but he does not own them.[102] If the person has these rights, and other persons appropriate them by any means they may be guilty of theft.

According to majority of Iraqi jurisprudence and UK legislation, the term 'belonging to

[99] Iraqi Penal Code 111 of 1969
[100] Section 223.0 (7) of the Model Penal Code 1962
[101] S 5(1)Theft Act 1968
[102] R Heaton, supra, note 3, 294

another' does not refer to the ownership only as the term is normally understood. However, it extends beyond the boundaries of possession and control.[103] Consequently, 'belonging to' refers to any possession or control of the thing by the possessor or the controller irrespective of whether the possession is legal or illegal. Therefore, a criminal may steal from several persons, such as the owner himself, possessor, or the individual who has a physical control of it.[104] More so, even the owner may be guilty of theft if he appropriates his property from the possessor or controller.[105] The thief may also steal property that in possession of another thief. For example, a second thief may appropriate the item that the first thief has previously stolen.[106] This also means that the possession or control that is mentioned in the Iraqi academic's literature and the UK legislation as a condition of a thing to be subject to criminal protection does not necessarily need to be lawful.[107]

The property sometimes does not belong to anyone, such as abandoned property, and then it cannot be the subject of theft. Therefore, if a person appropriates the abandoned property or the property that is not owned by any person he may not be guilty of theft.[108]

4.3.1.1 Abandoned Property

'Abandoned property' means a property that has been left alone and is not be used by its owner. On the other hand, it means 'a property where the owner has stopped carrying out at least one of the significant responsibilities of the ownership of property, as a result of which the property is vacant, or likely to become vacant in the immediate future.'[109] This type of property is deemed not to be property belonging to another.[110] However, it is worthy to state that not every property left *outside its place*, seems to have been entirely abandoned. Consequently, certain properties, such as property found

[103] *R v Woodman* [1974] QB 754 (CA)
[104] M Jefferson, supra, note 46, 608
[105] M Jefferson, ibid, 608
[106] *R v Meech* [1974] QB 549
[107] *R v Kelly* [1999] QB 621; M Jefferson, supra, note 46, 611
[108] R Heaton, supra, note 3, 294
[109] A Mallach, *Bringing Buildings Back*: *From Abandoned Properties to Community Assets* (Rutgers University Press 2005) 1
[110] S P Green, 'Theft by Omission' 2009, 1-18, Rutgers School of Law- Newark Research Report No. 050 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1410855> viewed on 12 February 2012

underground owned by a third party and a treasure trove are not considered abandoned property. The main requirements that may be required to consider the property as abandoned property are leaving the property alone should not be temporary[111] and the property should become useless property. Therefore, if a person 'takes' or 'carries' this property away he may not be guilty of theft. Abandoned properties give rise to the issue whether the lost, mislaid and unclaimed properties are considered types of abandoned property.

4.3.1.2 Lost Property

'Lost property' can be defined as property that the owner has involuntarily parted with[112] through neglect, carelessness, or inadvertence. For instance, if a wallet or money falls through a hole in a person's pocket, it is considered lost property. A main characteristic of this type of property is that the owner does not know where he can look for it. The law traditionally held that the owner of this type of property lost possession.[113] Consequently, if this type of property has been 'taken' or 'carried' away the accused may be guilty of theft.

4.3.1.3 Mislaid Property

'Mislaid property' is defined as property, which the owner has intentionally parted with.[114] The owner of mislaid property still has the possession of his property. Therefore, if someone 'takes' or 'carries' it away he may be guilty of theft.[115]

'Unclaimed property' the property is considered 'unclaimed property' if the owner does not claim it for some lengthy period of time. It is considered a type of tangible property, such as securities or cash. This property is found in banks or other institutions.

Dividing property into two types (lost and mislaid property) does not trigger a problem to the criminal law because the aim of this law is to reunite the owner with his lost property. The law obliges a person who finds lost or mislaid property to take reasonable

[111] S P Green, supra note 110, 15
[112] ibid, 15
[113] ibid, 16
[114] ibid
[115] ibid

steps to find its owner; otherwise, he may be guilty of theft. [116]

As a result, the property to be a subject of theft should belong to another person and it is not abandoned. The property should belong to the victim at the time of appropriation.[117] Accordingly, if the defendant appropriates another person's property at this time he may be guilty of theft. A question may arise regarding personal information; does personal information belong to another?

4.3.2 Scrutiny the Element of 'Belongs to Another' in Misuse of Personal Information

As mentioned in the previous section, a debate has arisen over whether personal information is property according to section 439 of theft offence laws 1969.[118] Consequently, personal information may or may not belong to another person depending on the result of this debate. For instance, if personal information is considered as property according to those who argue that it is property, then it can belong to another person and it may be a subject of theft. However, if is not it cannot belong to another person. Therefore, it cannot be a subject of theft under current legislation and jurisprudence.

As it is stated previously, personal information does not meet the elements of property that tangible property has been branded with. Personal information should be labelled as *fictional property*. The Iraqi legislature is requested to adopt the term of *fictional property* to protect personal and financial information of people from the act of the unlawful obtaining, and then using to commit other crimes. As a result, it could be said that people have authority on the information that they use to identify themselves. Consequently, it belongs to them, and it may be a subject of theft. To accomplish the above suggestion the Iraqi legislature is requested to enact a specific law, in which personal information is expressly considered as a specific type of property.

The Iraqi legislature is also requested to state expressly that personal information is *fictional property* and it belongs to the person who has authority to use it irrespective of

---

[116] S 2 (c), ((c Theft Act 1968) (except where the property came to him as trustee or personal representative if he appropriates the property in the belief that the person to whom the property belongs cannot be discovered by taking reasonable steps.)

[117] R Heaton, supra, note 3, 295; A Reed and B Fitzpatrick, supra, note 25

[118] See p 7, 8 of this chapter

whether that person is alive or dead.

Consequently, any problem that may be caused by the element belonging to another will be solved. For instance, the problem that may be caused when a person dies can be solved by adopting the term of fictional property. The problem that can be imagined is if for example, the person died, and then somebody used his information, to whom does the information belong? If the answer is that it belongs to the deceased, how can someone interpret the case in which the courts consider the accused who takes the property of a deceased person after his/her death and before the property has been divided among heirs, is not guilty of theft? The reason behind this is that the corpse is not property. However, if it has been preserved in the laboratory for study or anything else, it may become property.[119] As a result of the above, personal information should be considered a specific type of property. It belongs to the person who has authority and right to use it and to prevent the use of it without his consent by other persons.

In this manner, personal information may be protected to facilitate transactions among individuals and settle it. In addition, it may help to protect the information of the deceased because it is not necessary that *fictional property* meets the real elements of property.

Some people may relinquish their information, such as an old password or credit card number and not use it again. According to the general rule, this information is considered as abandoned information and it does not belong to another person. Consequently, if a person appropriates it he may not be guilty of identity theft. However, it might be said that to settle and facilitate transactions between people personal information should never be considered abandoned and any use of it to obtain illegal ends consists identity theft. It also should always belong to the person who has a right to use it. In addition, the person's consent to use his information to accomplish illegal ends should not be taken into account.

After assessing the longstanding debate on whether the elements of *actus reus* and property of theft offences are adequate to be applied to identity theft, it could be said

[119] M Jefferson, supra, note 46; *R v. Kelly* [1998] 3 All ER 741, CA; R Heaton, supra, note 3, 292; M J Allen and S Cooper, *Elliot and Wood's Cases and Material on Criminal Law* (10th edn London Sweet and Maxwell 2010) 632

that these elements give rise to difficulties. These difficulties might be solved by either a decision of court or specific legislation. However, even if these difficulties have been answered another obstacle may arise and obstruct applying the current Iraqi theft offence laws to identity theft. This obstacle is does using or taking another person's information away without his consent lead to permanently deprive him of his information?

4.4 *Mens Rea*

A general idea about the element of *mens rea* of theft will be given before the research goes to scrutinise the difficulties that may be faced when it is applied to the crime of identity theft.

4.4.1 General Concept of *Mens Rea*

The mental state of the accused is more important to determine whether he is guilty of theft. A person may not be guilty of theft even if he appropriates property belonging to another, if he has no intent to permanently depriving the owner of his property or his conduct is honest. In section 439 of theft offence laws 1969, The Iraqi legislature neither defines the *mens rea* of theft offence nor determines its elements. It only states that (theft is intentional appropriation of property ….). 'Intentional' is the *mens rea* of theft according to this section,[120] while in the UK legislation the legislature determines the elements of *mens rea*, but it does not utterly define the term of dishonesty.[121] According to the UK legislation, the elements of *mens rea* are dishonesty and intention to permanently deprive the owner of his property.[122] The US legislature in section 223.2 (1) states that 'a person is guilty of theft if he unlawfully takes, or exercises unlawful control over movable property of another person with purpose to deprive him thereof it'. According to this definition, the *mens re*a consists of two elements: (1) unlawful taking or exercising control over property and (2) deprive the owner of his property.[123]

---

[120] According to the public criminal provisions 'intentionally' means an intention to commit crime. It consists of two elements knowing and intention to commit crime.
[121] S 2 of the Theft Act 1968 c. 60 (UK)
[122] S 1 of the Theft Act 1968 UK ibid
[123] Section 223.2 (1) of the Model Penal Code US, in section 223.0 (1), the US legislature defines deprive as "deprive" 'means: (a) to withhold property of another permanently or for so extended a period as to

Iraqi scholars and judges believe that the *mens rea* means knowingly appropriation another person's property with intent to permanently deprive him of his property. The *mens rea* of theft consists of two elements: (1) knowingly and (2) intent to permanently deprive the owner of his property. These two elements will be discussed below.

4.4.2 Knowing and Willing to Commit Crime

As stated above, in theft offence laws the Iraqi legislature neither defines the element of *mens rea* nor determines its elements. Therefore, to define and determine the element of *mens rea* one should return to public provisions. According to these provisions, the term *mens rea* consists of three elements knowing, willing, and intent to commit crime. In this section, the elements knowing and willing to commit crime will be discussed.

Elements knowing and willing mean that the criminal knows that he commits an illegal act and wills to commit it. He should know that this act is prohibited by the law. As a result, the criminal lacks the *mens rea* to commit crime if he does not know that the act that he has committed is prohibited by the law or he knows that the act is prohibited, but he is forced to commit it. The Iraqi legislator does not adopt a specific standard to determine whether the criminal's act is honest or dishonest. The Iraqi criminal judge may consider the person guilty of a crime merely he commits an unlawful act.

Contrary to Iraqi legislator, the UK legislator in the Theft Act 1968 expressly states the term 'dishonesty' as a standard to determine whether the criminal's act is dishonest or not, but it does not completely define it. It defines it partly, when it creates a general frame of dishonesty or exceptions to it,[124] which do not explain the term dishonesty. The UK courts depend on two standards to determine whether the accused's act is dishonest. These standards are the common standards or the ordinary decent people

---

appropriate a major portion of its economic value, or with intent to restore only upon payment of reward or other compensation…'

[124] S 2 of the Theft Act 1968 UK; R Heaton, supra, note 3, 311; Exceptions that are provided by the UK's Theft Act of 1968 provide that the accused's conduct is not dishonest if his conduct enters within the scope of one of those exceptions. These exceptions are: the person believes that he has a right to deprive the owner of his property, the person believe that the owner would consent to the defendant taking his property or he believe that the owner would not be found by taking reasonable steps.

standard and secondly the accused's judgement or what the accused believed.[125]

According to above definition, the person may be guilty of identity theft if he knows that he uses another person's means of identification, and that person does not consent his means of identification being taken. However, if he does not know that the means of identification belongs to another person or he believes that the person consented to his means of identification being taken he may not be guilty of identity theft.

It could be said that the terms 'knowledge, dishonesty or willingness' as elements of *mens rea* gives rise to an issue regarding whether a person is guilty of identity theft or not because they relate to the person's state of mind. They are used to distinguish between the lawful and unlawful activities.[126] They are of no importance in determining the kind of crime. As a result, they do not trigger any difficulty with respect to applying the Iraqi theft offence laws to identity theft. These terms have no relationship with people's personal or financial information, whether it is property or not. In addition, they do not affect the *actus reus* occurrence. They affect the *mens rea* occurrence only. Therefore, if the person knowingly and willingly and dishonestly takes another person's information, and then uses it to commit other crimes, he may be guilty of identity theft. However, a person who knowingly uses another person's information without his consent may not be guilty of theft unless another element (such as 'an intention to permanently deprive the person of his/her information') takes place.

4.4.3 An Intention to Permanently Deprive the Owner of His Property:-

It is important giving a general idea about the element of permanently depriving the owner of his property and then scrutinise challenges that may be faced when it is applied to identity theft.

---

[125] According to common standards, the dishonesty of accused's conduct is the answer to the question 'Was that which the accused did dishonest by common standards?' If the answer is 'yes', then the defendant may be guilty of theft. However, if the answer is 'no', then the defendant may not be guilty of theft. While in what the accused believed standard it is an answer to the question 'Did the accused believe that what he did was dishonest or honest by common standards?' If the answer is 'yes', then the accused may be guilty of theft. However, if the answer is 'no', then the accused may not be guilty of theft. *R v Ghosh* [1982] QB 1053

[126] M Jefferson, supra, note 46, 581

4.4.3.1 Concept of the Element in Traditional Theft Offences

In section 439 of theft offence laws of 1969, the Iraqi legislature does not expressly state the element of 'an intention to permanently deprive the owner of his property.' it just states that theft is intentionally appropriating another person property. Scholars and judges in Iraq construe the term 'intentionally' to encompass 'an intention to permanently deprive,' whereas the UK and US legislatures expressly state this element in their legislation.[127]

Since the current Iraqi theft offence laws do not define the element of 'an intention to permanently deprive' and determine its features it is important to refer to the definitions that were held by the courts and jurisprudence to define it and draw its features. It is said that the owner is deprived of his property and the accused may be guilty of theft, if he appropriates any of the owner's rights over his property, even if the owner does not lose the thing itself.[128] For example, a person may be guilty of theft, if he deals with the thing as his own, such as he rents, borrows, or lends it, regardless of the owner's rights.[129] In other words, he intends to treat the property that he appropriates as his own, or to dispose of it, irrespective of the owner's rights,[130] or he deals with it in such way that he knows that he is risking its loss.[131]

Additionally, destroying or burning another person's property may satisfy the element of intending to permanently deprive. As a result, a person may be guilty of theft even though he does not take another person's property, but he destroys or burns it.[132] However, Iraqi jurisprudence and courts agreed with the UK legislature that using the thing for a period of time does not amount to permanently depriving the owner of his/her property[133] and a person may not be guilty of theft[134] because he intends to return the property to the person to whom it belongs.

---

[127] Section 223.0 (1), 223.2.(1) of the US Model Penal Code 1962; of the Theft Act of 1968 s 6(1)
[128] M Jefferson, supra, note 46, 581
[129] R Heaton, supra, note 3, 318; *R v. Cahill* [1993] Crim LR 141, CA
[130] R Heaton, ibid, 319
[131] *R v Fernandes* [1996] 1 Cr App R 175
[132] M Jefferson, supra, note 46, 581; in the Iraqi legislation if the property is not removed from its place and destroyed or burned in the same place, it does not constitute theft. See Article 374 of the Iraqi Penal Code 111 of 1969.
[133] S 6(1) Theft Act of 1968
[134] D Ormerod supra, note 25, 788; *Neal v Gribble* [1978] RTR 409

The perpetrator may have an intention to commit theft, in other words, he had criminal intention or criminal liability to commit theft, or he may have committed it recklessly. Recklessness is an act that is committed by a perpetrator and contains no intention to commit crime.[135] The state of recklessness is not found in the UK, US and Iraqi legislation. However, the Canadian legislation mentions it as a means to commit theft. Therefore, the courts in these countries may apply general criminal rules to the person who recklessly commits theft.[136] It is possible to say that the Iraqi legislator is recommended to place recklessness in its legislation.

The question remains whether the current Iraqi theft offence laws can be applied to a person, who knowingly gets, hears or sees another person's means of identification, and then memorises it to use this information to accomplish illegal ends, such as committing fraud or obtaining benefit from the government. In other words, is there permanent deprivation to the person of his information, when the accused uses it without the person's consent?

4.4.3.2 An Evaluation of an Intention to Permanently Deprive in Identity Theft

The specific nature of personal information causes a debate between scholars as well as judges whether there is permanent depriving to the owner of his information in identity theft. Therefore, it is more important to assess this argument and draw the features of this element.

According to the first camp of debate, it is argued that even if there is no deprivation to the owner when his information illegally has been used, the use of it by others and without his consent may decrease its value. Decreasing the value of the information refers to depriving the owner of it.[137] Moreover, it is pointed out that there is no

[135] M R Berry, 'Does Delaware's Section 102(b) (7) Protects Reckless Director from Personal Liability? Only if Delaware Courts Act in Good Faith' (2004) Vol.79 Law Journal Library Washington Law Review 1125-1153

[136] The Iraqi legislation does not take into account the term recklessness as a means to commit intentional crimes. It takes in account when a person wrongly causes another person death, Article 411 of Iraqi Penal Code 1969

[137] S W Branner, supra, note 69, 12; Hardan claimed that taking of another person's means of identification permanently deprives the owner of it. In this case, the accused may be prosecuted on theft according to article 439 of the Penal Code 1969, fraud or betrayal trust when the accused take his fellow's means of identification or the means of any person who has relationship with him, interview

difference between the use of tangible property, such as a battery and the use of another person's information, and the decrease in its value; both should be guilty of theft.[138] As a result, some scholars[139] equate the use of another person's information and the use of his physical property without his consent. They state that there is permanently depriving the owner of his property in both case, because the accused also uses the information as his own property irrespective of the owner's rights.

However, it has been said that the application of the *mens rea* of theft offences to *identity theft* may be faced by many obstacles.[140] For instance, it has been said that there is no permanent deprivation to the person, whose information, such as mother's maiden name, date of birth or address has been taken, of it because he still uses this information. Accordingly, the element of the intention to permanently deprive cannot be applied to a person who takes or uses another person's information without his consent. The real issue is that the owner has been forced to share his/her information with others. After all, the peculiar nature of information is that it allows more than one person to use it.[141] Moreover, sharing information does not change the nature and the content of information.[142] Sharing information may decrease the value of the property, but neither does the information lose its value, nor does the sharing deprive the owner of it.[143]

In the Victoria case (*Akbulut v Grimeshaw*);[144] the court stated some facts to confirm that the use of personal information of another person does not satisfy the element of permanent deprivation of the owner of his property. The judge in this case stated that the accused had made unauthorised phone calls under the victim's name, but did not commit theft of service. Thus, he is not guilty of theft of service. The judge reasoned

---

with Ali Hardan the Head of Diyala Criminal Court, Presidency of the Federal Court of Appeal of Diyala (Diyala, 5 February 2013)

[138] C R Davies, supra, note 47, 409

[139] M Al-Shawa, supra, note 56, 65; A Tammam, supra, note 9, 482

[140] A Reed and B Fitzpatrick, supra, note 25, 476

[141] *R .v. Offley* 1986), 70 A.R. 365

[142] A Endeshaw, 'Theft of Information Revisited' (1997) Vol.187 Journal of Business Law 1-7

[143] J Cross, supra, note 19, 265; A L Christie, supra, note 6, 353; Obeidi claimed that taking of another person's means of identification does not permanently deprive him of it, interview with Bidoor Obeidi, a prosecutor at Presidency of the Federal Court of Appeal of Diyala (Diyala, 26 January 2013); Maeen claimed that taking another person's means of identification does not permanently deprive him of it, interview with Jawad Khalid Maeen, the Head of the first criminal group at Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

[144] *Akbulut v. Grimeshaw* 96 A Crim R [1991]

that ‘there is no property vested in the owner which is capable of being appropriated before the act, which was the telephone calls’, and the owner was not deprived of his/her property.[145] The only thing that the perpetrator did was share the phone with the owner, which, in turn resulted in additional cost to the owner.[146]

In the same vein, the Canadian Supreme Court asserted in *R v Stewart*[147] that there is one state in which the owner of information might suffer deprivation, if he lost the confidentiality. The court however stated that even in this state the information could not be considered a subject of theft because no one can own the confidentiality, although he enjoys it. Therefore, the usage of the person’s confidential information without his consent does not therefore deprive him of his information. The Canadian Supreme Court confirmed a decision was held in *R v. Offley.*[148] In this case, the court pointed out that there is no permanent deprivation to the owner of his/her information when it has been used by another person because the owner of the information still retains, possesses and uses it. As a result, if the accuser, for instance, hears or sees the person when he/she gives his/her information to another person via telephone or enters it in the ATM, and then he uses it to accomplish illegal ends, there is no physical thing that has been taken. The owner also is not deprived of his/her information because the owner can continue to use or possess it.[149]

It can be said that, undoubtedly, the use of one person’s information by another person without consent to obtain illegal ends is illegal and immoral behaviour. However, this use does not amount to permanently deprive the owner of his information. In fact, the owner of the information continues to use it as if there is no appropriation occurred. Consequently, the *mens rea* of theft offences cannot apply to the use of another person’s information without his consent and the Iraqi legislature is requested to enact a specific Act to define and determine the *mens rea* of identity theft.

Having the longstanding argument regarding difficulties that may be encountered when Iraqi theft offence laws are applied to identity theft has been examined, it seems that

[145] *Akbulut v. Grimshaw* [1998] 3 VR 756
[146] ibid; A Steel, supra, note 16, 557
[147] *R. v. Stewart*, supra
[148] *R .v. Offley* 1986), supra
[149] C J Dickson, et al, supra, note 21, 20; M Shawabkeh, supra, note 12, 143; Ateek, supra, note 13; J Esseqair, supra, note 12, 103

these difficulties are found and obstruct the application of these laws to identity theft. These difficulties should be solved by either the courts setting new decisions or the legislation enacting reform. The legislature in this legislative reform should address identity theft as a means that can be used to facilitate other crimes occurrence or address it as a new specific kind of theft. If the legislature considers identity theft a specific kind of theft, it should define the *actus reus* and *mens rea* of identity theft. As a result, this study suggests the proposed *actus reus*.

4.5 Proposed *Actus Reus* of Identity Theft

4.5.1 *Actus Reus*

Actus reus as an element of identity theft is either a legal or an illegal activity whether sophisticated or non-sophisticated that is committed by a person to acquire a means of identification of another person, and then use it to commit other crimes. It as the *actus reus* of theft consists of elements[150]: an illegal or a legal activity. The author will also propose the subject matter of identity theft, which consists of a means of identification that belongs to another.

4.5.1.1 An Illegal or a Legal Activity

An 'activity' is an act by which a person can acquire another person's means of identification,[151] such as seeing or hearing it and then memorising it in order to commit other crimes. As it provided previously, personal information is an intangible thing. It cannot be subject to physical taking. Therefore, the criminal can use any method whether physical or non-physical to obtain this information (such as assuming, seeing or hearing this information and then memorise it to use for illicit ends).[152] Criminals may use two methods to obtain another person's means of identification: (1) traditional

---

[150] C Elliott and F Quinn, *Criminal Law* (8th edn London Hinry Ling Ltd Dorset Press Dorset 2010) 193

[151] The US legislature in section (c) of 1028 a (7) considers identity theft as a crime and defines it as a person may be guilty if he Knowingly transfers, uses, …….a means of identification of another person ……., the *actus reus* of identity theft according to this act is transferring or use a means of another person; the Canadian legislature in s 4 defines identity theft as knowingly obtaining or possession another person's identity information in circumstance giving rise to a reasonable interference that this information intend to be used….. In addition, it mentions that a person may be guilty of an offence if he transmits, makes, distributes, sells or offer for sale another person's identity information …

[152] D Marron, 'Alter Reality: Governing the Risk of Identity Theft'(2008) Vol. 48 British Journal of Criminology 20-38

(such as wallet or purse theft, mailbox theft, searching in a waste bin, or theft inside work) and (2) non-traditional or sophisticated methods (such as phishing, spam, viruses, and Trojan Horse). Some of the sophisticated methods stand alone as crimes. Accordingly, they need specific legislation to be criminalised.

Contrary to the US legislature who, as it will be shown, punishes identity theft criminals if they transfer or use the stolen information to commit other crimes only, the Iraqi legislature is requested to criminalise the act of both the legal and illegal obtaining of personal information and then using it to their purposes. It is also requested to criminalise the means that may be used to obtain this information and it is considered a crime in itself, such as phishing or spam. In addition, the Iraqi legislature is requested to criminalise the use of; transfer of personal information, sale, offer for sale, distributing and making the use of personal or financial information of another person available for others.

The above suggestion can be endorsed by many facts; on the one hand, the process of information exchange may be more secure if the person who steals the information with intention to accomplish illegal ends has been punished, even if he does not use this information to commit other crimes. Punishing the accused at this stage may be considered to be measures to counter the dangerous criminals and gang groups, particularly; with the internet, identity theft has become a global crime.

On the other hand, most crimes that are committed or facilitated by using stolen information relate to financial crimes, thus, if someone uses this information to accomplish illegal ends he may be guilty of an aggravated crime, such as fraud or receiving medical care. However, if he does not use this information to commit other crimes, he may be guilty of identity theft only. Possession of personal information of another person resembles the possession of an artificial key or a weapon, without permission, that may be used to facilitate other crimes. The artificial key, which is considered a means to facilitate theft or other crimes commission, has been criminalised by most legislatures, such as Iraqi legislation. Consequently, identity theft should be criminalised as the artificial key.

4.5.2 An Identity or a Means of Identification

An identity is a complex and an ambiguous term.[153] There is no definite definition for it. It is used in different fields to distinguish between individuals, to describe the relationship between individuals and the State, or to describe specific groups. Therefore, it has many names, elements and different structure. It may be named a gender identity, personal identity, national identity, or ethnic identity.

Scholars and professionals use the term identity to express many things. However, it can be used to refer to two main things that are always used between academics and individuals: National identity and personal identity.[154] The main concept of identity that concerns this study is the personal identity or so called a means of identification of a person.

There are many definitions of personal identity. For instance, Jenkins[155] defines it as a way in which individuals and collectivities can be distinguished in their social. Personal identity can also be defined as 'an actor attributes to itself while taking the respective the other that is, as a social object...or it is cognitive schemas that enable an actor to determine who I'm/we are in situation and position in social role structure of shared understandings and expectation'.[156] The US legislature in section 3 of the Identity Theft Act 1998 defines it as 'any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual'.[157]

As it noticed in the previous chapter, criminals may target individuals, companies, or institutions of state, therefore, identity can be defined as a set of characteristics, symbols, numbers, or elements in which individuals or groups distinguish each other and they act in a manner to respect each other. Identity consists of many elements that are used to distinguish individuals, such as names, addresses, or passwords. Individuals have a right to use any means of identification to define themselves.

---

[153] D James Fearon, 'What Is Identity (as We Now Use the Word)' 1999 1 available at <http://www.stanford.edu/~jfearon/papers/iden1v2.pdf> viewed on 30 March 2012

[154] R Jenkins, 'Categorization: Identity, Social Process and Epistemology' (2000) Vol. 43 (3) Current Sociology 7-25

[155] ibid, 12

[156] A Wendt, 'Collective Identity Formation and the International State' (1994) Vol. 88 (2) American Political Science Review 384-396

[157] S (c) (3) (C) Identity Theft and Assumption Deterrence Act of 1998

In effect, people always use their names as a means to identify themselves. However, the name as a means of identification may raise many problems because many people have the same name. Accordingly, it is very difficult to distinguish between people by using names only. In addition, some people use more than one name in their life and that may make the distinction between them impossible. As a result, a person should use another element with his name to enhance it, such as social security number, password, or driving license. Consequently, the Iraqi legislature is requested to take these elements into account when it defines identity of a person that may be subject to theft. The Iraqi legislature can adopt the definition that is proposed by this research or adopt the definition that is found in the US Identity Theft Act 1998.

If any means of identification, such as a name, address or driving license number has been used alone or in conjunction with any other information by the person to define himself he has a right to use this means and prevent other people from using it without his consent. In other words, the means of identification that is used by a person to distinguish himself belongs to that person and taking it without his consent constitutes an offence.

4.5.3 Belonging to Another

A means of identification, such as names, addresses, passwords, credit card numbers, mother's maiden name, social security numbers, and PIN numbers as a subject of theft should belong to the person who has a right to use it. The term 'another' means any person whether he is alive or dead. In addition, it may refer to the legal person because the identity of the legal person may also be a subject of theft.

Personal identity or a means of identification of another person is more vulnerable to risk and misuses by other people. It has become more important in current life. As a result, some people seek to obtain this means of identification, and then use it to commit other crimes (such as fraud or terrorism). Therefore, the Iraqi legislature is requested to adopt the above elements of *actus reus* if it intends to enact a new Act to protect personal or financial information.

If the means of identification does not belong to another person, it may be a false means of identification or it is considered an abandoned means. Consequently, if this

means of identification has been taken by a person he may not be guilty of identity theft. As it is stated previously, any identifier that has been used by the person to define himself should not be considered abandoned and the use of it without consent to accomplish illegal ends should be criminalised. However, it could be said that a person's means of identification, such as his past address, password and other means of identification that is not in use, may not belong to that person unless it used with his current means of identification, such as his name or credit card details.

An issue may be branded more important than another issue and needs to be discussed in more detail. This issue is if the Iraqi legislature does not enter to find a solution to this problem or the processes of the enactment of the new law take a long time, can the judge extend existing theft offence laws or create a new law or crime to include the misuse of the personal information. This issue will be discussed in the next chapter.

4.6 Conclusion

An important issue has been addressed in this chapter, namely, whether existing theft offence laws in Iraq are adequate to govern identity theft. In other words, the issue that has been addressed is to appreciate whether a crime of identity theft falls within the scope of traditional theft. To clarify whether or not the traditional rules are adequate, the chapter has been divided into four sections and some subsections.

The first section deals with the *actus reus*. It was shown that the *actus reus* of theft offences consists of the element 'appropriation'. Both sections two and three deal with property and belonging to another. These three elements (appropriation, property and belonging to another) raised difficulties to apply the current Iraqi theft offence laws to identity theft. Therefore, a fervent argument has risen in the empirical literature with respect to these elements, whether they exist in the *actus reus* of identity theft.

A debate arose with respect to the term or element of appropriation. The debate formed two groups. One group believes that the element of appropriation does not satisfy the element of offence of identity theft because personal information cannot be taken or carried away like physical property. However, other scholars criticise this view and point out that the element of appropriation can satisfy the method that is used to commit identity theft. The study showed that the element of appropriation is inadequate to

encompass the methods that are used to commit identity.

The argument among scholars also extended to encompass the analysis of whether personal information is property. Some scholars believe that personal information is property and it may be subject to theft. Others believe that personal information is not property. Accordingly, it cannot be subject to theft. As a result of this argument, the study examined how the UK and the US courts tried to justify that personal information is property through the concept of property in the civil law.

Two different approaches are used by the US and the UK courts. It was shown that the UK courts adopt breach of confidence (contract or equity) and the fiduciary contract approaches, whereas US courts adopted the property theory and equity or obligation approach. These courts intended, by adopting these approaches, to transfer the concept of property from civil law to criminal law. The study showed that there is a difficulty regarding the use of the concept of property that is found in civil law within the scope of criminal law because there are many differences between the two laws. As a result, Iraqi courts cannot adopt each of these approaches to determine whether personal or financial information is property.

With respect to the element of belonging to another, there is no problem that may arise when existing theft offence laws in Iraq are applied to identity theft because this element depends on the result of the debate relates to whether personal information is property. As a result, personal information may belong to another person if it is considered as property. The author believes that if personal information is considered by the court or legislator as property, it always belongs to the person who has authority to use it.

The current study showed that to provide an adequate protection to personal or financial information of people, this information should not be considered as abandoned information. However, some information, such as the past address or password may be considered abandoned and use it without consent does not constitute a crime unless it has been used with another means of identification, such as the person's name or his credit card number.

Section four contains the discussion that is conducted by the author and relates to the

m*ens rea*. In this discussion, it was shown that the m*ens rea* of theft offence consists of two elements: knowledge and an intention to permanently deprive the owner of his property. It also showed that the element 'knowledge' does not give rise to a problem with respect to the application of existing Iraqi theft offence laws to identity theft because the element of 'knowledge' describes only whether the accused's act is legal or not. Conversely, the element of an intention to permanently deprive the owner of his property gives rise to a deep debate between scholars and professionals.

The debate focussed on whether the use of another person's information without consent causes permanent deprivation to him of his information. Some scholars state that the use of the personal information of another person deprives him of his information. However, other scholars state that the use of another person's information without consent does not deprive him of it. The author has upheld the view of the debate, which believes that the element of intention to permanently deprive the owner of his property cannot meet the *mens rea* that may available to identity theft because the owner is not permanently deprived of his information and he still uses and enjoined it.

It was shown that traditional elements of theft do not exist in the crime of identity theft. Accordingly, existing Iraqi theft laws are inadequate to govern identity theft and this inadequacy in the legislation should be solved by either a decision from the court or by the legislature through enacting new Acts to govern identity theft. Finally, in section five, the author defined the potential *actus reus* of identity theft that may be adopted by the Iraqi legislation.

The next chapter looks at explanations concerning the issue whether the Iraqi criminal judge can extend the current theft offence laws or create a new law to govern identity theft.

Chapter Five:

A Judicial Solution to Plug the Legislative Inadequacy to Combat Identity Theft?

Introduction

As already noted in the previous chapter, existing theft offence laws in Iraq are inadequate to govern identity theft because these laws have been enacted to deal with and protect moveable material property only, whereas a person's means of identification, which may be subject to theft, has a specific nature. It is intangible. This inadequacy gave rise to many difficulties that were examined and determined in the previous chapter. These difficulties might prevent the application of existing theft offence laws in Iraq to identity theft. Consequently, a solution should be provided to overcome these difficulties (or enact a new law) to combat this type of crime. As many scholars and judges believe that this solution should be provided by either a competent court or the legislature.

Owing to the enactment of the law pass across many series of the processes, it may take a long time. Therefore, a judicial solution sometimes becomes an urgent issue. The judicial solution may be better than the legislative solution because it does not pass in a long series of processes that the legislation passes in them. In this chapter, the focus will be on the potential judicial solution to overcome the legislative inadequacy of the existing theft offence laws to combat identity theft, which has been determined in chapter four.

In most countries, judges can overcome any inadequacy that may be found in their legislation by either the interpretation of the statute or by the analogy. Consequently, Iraqi criminal judges like those judges may overcome the legislative inadequacy of the current theft offence laws, which has been determined in the previous chapter by either interpreting these laws or analogy. To examine whether Iraqi judges can achieve this commission and overcome the legislative inadequacy, the elements of theft offences will be analysed. The researcher also invited the experience of US and UK jurisdictions to make an analysis of the findings and thereafter to provide a proper position about the method in which these difficulties can be accommodated in the current Iraqi theft

offence laws.

However, the role of the Iraqi judge to fill the gap that is found in the current theft offence laws through the above two methods may be obstructed by the principle of legality that is set forth in Iraqi legislation. To assess whether the principle of legality curbs judges to find a solution to overcome the legislation inadequacy, a brief idea about the principle of legality will also be given in this chapter. Therefore, this chapter will be divided into three main sections: section one includes the clarifications of the methods that are used to interpret existing theft offence laws. Section two deals with obstacles that may prevent the judicial solution to overcome the legislative inadequacy and in the final section, the role of Iraqi judges to interpret the current theft offence laws and expand their scope to cover identity theft will be examined.

5.1 Interpreting Iraqi Legislation

There is no legislation in the world can be enacted in advance to govern all eventualities because legislatures may not predict some events; and life is constantly changing.[1] Therefore, judges are still having a central role to play in shaping the law. In addition, even if legislation governs existing unlawful activities, it may be ambiguous and unclear. Consequently, judges sometimes attempt to interpret the statute to explore the spirit of it or to plug any gaps that may appear in it.[2] In most countries, there are two methods that can be used to close such gaps: extending the existing law through interpretation (or creating a new law).

[1] R Huxley-Binns and J Martin, *Unlocking the English Leagal System* (3rd edn, Hodder Education 2010) 57; L Cherkassky, et al, *Legal Skills* (Palgrave Mamillan 2011)

[2] The interpretation of the statute can also be conducted by legislators and idiosyncratic. Thus, the interpretation is divided into two types according to the authority that interprets the legislation: the legislative interpretation and idiosyncratic interpretation. The legislative interpretation means the legislator sometime explains the meaning of some terminologies that are found in the acts. It may be in the same Act, for instance, the UK legislature in the Police and Criminal Evidence Act 1984 provides interpretation sections in the end of the Act that explain some of the words. On the other hand, the legislator may provide the courts with some guidance sources that explain some terminologies, which have been stated in the statutory. For example, in the interpretation Act of 1978, the UK legislature provides some standards, which explain the meaning of some words, such as singular, include plural and 'he' include 'she'. The jurisprudence has considered more important vector to develop criminal laws and determine the strong and the weakness points of legislation. The indeterminacy language that associated with the legislation makes it unclear, incomplete, and ambiguous. Accordingly, it should be interpreted. The jurisprudence one of many parties may interpret the legislation to determine that it is certain enough and warning the potential perpetrators in adequate and certain methods. As well, it is considered as a guide for individuals to avoid and do not violate it. Contrary, the jurisprudence interpretation may prove that legislation is inadequate and it needs to be modified to deter criminals. The jurisprudence interpretation does not abide the legislator or the judge.

The question remains can the Iraqi criminal judge as if most countries interpret existing theft offence laws in a manner that governs identity theft (or create a new law) to govern identity theft. To answer the above question, methods that may be used to interpret existing theft offence laws will be discussed below.

5.1.0 Types of Judicial Interpretation of a Statute:-

The interpretation of the statute becomes a part of it once it has been accomplished by judges.[3] In addition, the interpretation subjects to the same rules that are applied to the statutory. All courts whether civil or criminal have rights to construe the ambiguous legislation when they intend to apply it. However, the higher court only has a right to determine whether the lower court's interpretation of legislation is correct or not. Moreover, it has a right to overrule the lower court's interpretation in the same case if the case has been come before it or overrule it in a later case. In the latter instance (overruling the lower court's decision by the higher court), the lower court will continue in its interpretation until the higher court overrules its interpretation.[4] The higher court also may have the right to fill in the gap that may be found in the legislation. Three types of methods can be used by judges to interpret laws: (1) literal interpretation, (2) the expansive interpretation, and (3) the discovery approach. To scrutinise whether Iraqi criminal judges represented by Federal Court Cassation's judges can fill in the gap in the current theft offence laws, and if they can, how they close this gap, the above types of interpretation will be discussed below:

5.1.1 Narrow Interpretation or Literal Interpretation

Narrow interpretation means 'the application of criminal statute is limited to the hard core of the meaning that almost any reader would derive from a statute'.[5] If the statute is clear and unambiguous, the judge gives the words their normal meaning when he

---

[3] RS Geddes, 'Purpose and Context in Statutory Interpretation' 127-157 available at <http://www.judcom.nsw.gov.au/publications/education-monographs-1/monograph4/07_geddes.pdf> viewed on 10 January 2012

[4] C Elliott and F Quinn, *English Legal System* (11th edn, Pearson Education Limited London 2010) 54

[5] K S Gallant, 'The Principle of Legality in International and Comparative Criminal Law' (2007) 1-36 available at <http://www.gistprobono.org/sitebuildercontent/sitebuilderfiles/internationalcomparativecriminallaw306.pdf> accessed on 22 April 2011, 23; A Gillespie, *The English Legal System* (2nd edn, Oxford University Press 2009) 37

interprets the statute.[6] The judge gives the words of the statute their normal and natural meaning irrespective of whether the result is reasonable or not.[7] However, if the law is ambiguous the judge should interpret it in a manner that does not lead to expanding its meaning, or to creating a crime and its punishment.[8] As a result of the narrow approach, the judge cannot create a crime or punishment, even if the conduct of the accused is more dangerous and may affect society, if the current law does not consider this conduct as a crime, or it is considered a crime, but the punishment for it is insufficient.[9]

The literal interpretation is considered a result of the principles of the legislative supremacy of Parliament, the separation of powers and the rule of law.[10] As a result, the judge abides by the literal meaning of the law when he applies it. This result was confirmed, for instance, by a decision that was issued by the Iraqi Court of Cassation in *M v. K*.[11] In this case, the court stated that the garage could not be considered as a part of the home because it was not one of the types that were stated in section 443 of article 439 of theft offence laws.

In the same sense, both the US Supreme Court in *United States v. Brown* [12] and the UK Court in *R v. Goodwin*[13] confirmed that the judges should abide by the literal meaning of the statutes when they use the literal interpretation as a means to interpret the ambiguous statutes.

In *United States v. Brown,* the US Supreme Court stated:

> The canon in favor of strict construction [of criminal statutes] is not an inexorable command to override common sense and evident statutory purpose . . . Nor does it demand that a statute be given the "narrowest meaning"; it is satisfied if the words are given their fair meaning in ac-cord with the manifest intent of the lawmakers.

---

[6] *Boss Holdings v Grosvenor West End Properties* [2008] UKHL 5; *R v Environment Agency* [2007] UKHL 30; *A v. Adamiya Investigation Court* Iraqi Court of Cassation Civil Extended Commission [2010] 289

[7] C Elliott and F Quinn, supra, note 4, 54; M Zander, *The Law Making – Process* (6th edn, Law in Context CUP Cambridge 2004) 130; *R v Horsman* [1998] QB 531; *R v Smith* [2002] EWCA Crim 2907

[8] L Li, 'Nulla Poena Sine Lege in China: Rigidity or Flexibility?' 2010) Vol. 43 (3) Suffolk University Law Review 655-668

[9] ibid

[10] M Cremona, *Legal Method* (7th edn, Palgrave Macmilan United Kingdom 2009) 268

[11] *M v. K* [1970] Iraqi Court of Cassation 1648; see also *S v. H* [1971] Iraqi Court of Cassation J 1697; *A v. K* [1971] Iraqi Court of Cassation J 177

[12] *United States v. Brown* 333 U.S. 18 (68 S.Ct. 376, 92 L.Ed. 442) (1948)

[13] *R v Goodwin* [2005] EWCA Crim 3184

When the UK court attempted to construe section 58 (2) (a) of the Merchant Shipping Act 1995 in *R v Goodwin* it stated that Jet Ski could not be considered a ship because this section did not mention it as a type of ship.[14] In addition, In *R v Preddy*[15] the House of Lords espoused the literal rule to interpret legislation. In this case, the judge stated that it was unacceptable to consider the obtaining of mortgage by deception as a crime. To justify its decision the House of Lords stated that the transaction was performed when one chose in action was extinct and another one has been created in a different account. The new chose in action did not belong to the drawer. It belonged to the payee and so no 'property belonging to another' could be obtained by the payee with section 15(1).

A good advantage of the literal interpretation is it respects the sovereignty of the Parliament and prevents the domination of judges.[16] However, it cannot be accepted as a means to construe the ambiguous statute because it leads to isolate the judge from the environment and social self, whereas when the judge interprets the law he cannot separate himself from the environment and social self.[17] In addition, it may lead to undesirable and unsustainable consequences.[18] Moreover, it may lead to unfairness and harsh decisions.[19]

According to the concept of literal interpretation of statute that was determined above, the Iraqi criminal judge cannot use the literal interpretation to extend existing theft offence laws to overcome the inadequacy that is found within them because this type of interpretation obliges the judge to apply existing theft offence laws as they have been enacted. It does not allow the criminal judge to add or omit from these laws any term even if it is they are ambiguous.

It could be said that in the current theft offence laws, the Iraqi legislature does not define the *actus reus* and *mens rea* of theft, thus, they are ambiguous and unclear. However, even with this ambiguity Iraqi criminal judges cannot use the literal approach

[14] *R v Goodwin* [2005] supra
[15] [1996] AC 815
[16] M Alraezki, *Lectures in Criminal Law: (General Part) the General Principles-Crime-Criminal Liability (*3rd edn, Dar Oea, Tripoli 1999) 18
[17] E Ferri, *Criminal Sociology*, 227, (D. Appleton & Co. 1897) cited in L Li, supra, note 8
[18] C Elliott and F Quinn supra, note 4, 18
[19] R Ward and A Akhtar, *English Legal system* (11th end, Oxford University Press Inc. New York 2011) 65

to extend these laws to govern identity theft because this approach is limited to the application of theft offence laws to the core of their meaning that the ordinary person can understand.

In other words, the Iraqi judge cannot use the literal interpretation to extend existing theft offence laws (or create a new law) to govern identity theft. Consequently, Iraqi judges may look for another way to construe the current theft offence laws in order to extend them to cover identity theft. This way is the *extensive* approach.

5.1.2 Extensive Interpretation

Extensive interpretation means giving the legislation broad meaning by using the broadest actual denotation of its words[20] to discover the spirit of the legislation. Interpreting the law by judges according to this approach may lead to extend the existing law (or to create a new law). It also gives the law retroactive effects because the judge gives the legislation the broadest meaning of its words[21], which may allow the judge to apply this legislation to illegal activities that took place in the past. The extensive approach is more important to interpret the ambiguous statutes and close a gap that may be found in them. It may help the judge to achieve justice and ensure the development of the law.[22] For instance, in *K* and *others v. Muthanna Criminal Court*,[23] the majority in the Iraqi Court of Cassation stated that the life imprisonment equates capital punishment because the life imprisonment means killing the accused indirectly. Consequently, the punishment for inchoate of this crime is the prison for 25 years.

Nowadays, after US's invasion for the Iraq and many terrorists have entered to it, many crimes have been committed by using unknown means to the Iraqi legislature. As a result, Iraqi judges always require the interpretation of the law to determine the correct legal text that can be used to govern these unlawful activities.[24] The expansive

---

[20] K S Gallant, supra, note 5, 24

[21] *People v. Sobiek* 30 Cal. App. 3d 458 (1973)106 Cal. Rptr. 519

[22] E Ferri, supra, note 17, 227

[23] *K and other v. Muthanna Criminal Court* [2007] 173; in *A v. Criminal Centre Court*, Five Commission, the Iraqi Court of Cassation stated that the crime, which falls within the scope of Terrorism Act 2005, it also falls within the scope of the Amnesty Act No.19 of 2008 if it does not cause killing or permanent bodily harm. *A v. Criminal Centre Court*, Iraqi Court of Cassation Five Commission [2009] 178

[24] For instance, Hardan claimed that by now, terrorists use Chlorine in booms to kill people. The Chlorine is a legal material and its possession is not crime. However, it may be illegal means to commit crimes if it

interpretation is the best types of interpretation, which may be used by Iraqi criminal judges to interpret the statute.

Most interviewees[25] who were interviewed claimed that judges could use the expansive interpretation to explore the spirit of the statute, but they cannot create a new crime or set a punishment for it. On other hands, some of them[26] went further and claimed that judges by doing so could extend existing laws to govern the new unlawful activities without violating the principle of legality because new crimes are not created in this case. They stressed that these unlawful activities are traditional crimes committed using new methods. Judges do not take account of the ways used to commit crimes when they apply the law. They also claimed that judges focus only on the crimes that have been committed and then sentence the accused accordingly.

The author could not find decisions that may explain how the Iraqi judges can use the expansive interpretation to interpret existing theft offence laws. However, he has found decisions, but he observes that Iraqi courts do not state what kind of interpretation that they use to interpret the criminal statute and their discussion of evidence that is presented in the criminal cases are too short. These decisions cannot support his analyses to assess whether Iraqi judges can interpret the current theft laws in a sufficient manner to cover identity theft. As a result, he uses a decision that was issued by UK House of Lord to illustrate how the expansive approach can be used to interpret the ambiguous statute. For instance, the application of extensive approach can clearly be noticed in a decision that was taken by the House of Lords in *R v Hinks.*[27] The House of Lords interpreted the term 'appropriation' that is stated in the Theft Act 1968 and extended the scope of its meaning to include also giving a gift.

---

is used to make booms to kill people. The use of this new means to commit terrorist crimes was unpredictable for the Iraqi legislature when it enacted the Terrorism Act No. 13, 2005. Therefore, judges interpret the Terrorism Act to determine the illegal activity and the means that is used to commit it. Interview with A Hardan, the Head of Diyala Criminal Court, (Diyala, 5 February 2013).

[25] Interview with Dr. assist Professor Firas Abdul Moneim, the Head of law department at Baghdad University School of Law, (Baghdad, 20 February 2013); interview with Dr. assistant Professor Salah Al Fatlawi, a lecturer and Deputy Head of School of Law, Baghdad University School of Law (Baghdad, 16 February 2013); interview with J Khalid Maeen, the Head of the first criminal group at Appeal Baghdad Federal Court, Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

[26] Interview with A Al Obeidi, and A Al Ali lawyers at Presidency of the Federal Court of Appeal of Baghdad/ Rusafa (Baghdad, 27 February 2013); interview with M Abdul Ali, a judge at Presidency of Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

[27] [2001] 2 AC 241

Due to the extensive interpretation expands the meaning of the legislation, and leads to creating a new crime, increasing, or decreasing the punishment amount, some scholars[28] believe that literal interpretation is better than it. Nowadays, many States prefer the extensive interpretation, such as Denmark, Russia, China,[29] and most US states.

It could be said that the Iraqi criminal judge may use this type of interpretation to interpret the current theft offence laws and extend their scope to govern identity theft and plug the inadequacy that was determined in them in chapter four. Sometimes when the judges use the extensive interpretation they do not need to extend (or to create a new) law, they may interpret existing laws to explore the spirit of these laws. This type of interpretation is called the purposive approach.

5.1.3 Purposive Approach:

The purposive approach aims to bring out the purpose of the law irrespective of the literal meaning of the words of the law. It concentrates on providing the effect of the purpose of the statute. According to this approach, judges have to look for the intention of the legislature not to what the statute meant.[30] The goal of this approach is to find the spirit of the law even if it leads to some extent or to ignoring the literalism of the provisions.[31]

The purpose approach allows courts to deduce the intention of Parliament or the legislature from external materials[32] irrespective of whether the interpretation was literal or expansive approach.[33] Although most scholars and judges in Iraq have knowledge about this type of interpretation, the author has not found any decisions issued by the Iraqi Court of Cassation to illustrate how this court has interpreted criminal laws. In addition, the main problem that the author suffers from is when Iraqi judges interpret the statute they do not explain how they interpret the statute and why.

---

[28] K S Gallant, supra, note 5, 23; A Shamuon, *The National Plan for Human Rights- The Right in Living, Lebanon Parliament Council* (without a year publishing); 455-522; *United States v. Rodgers* 706 F .2d 854 (8th Cir. 1983)

[29] J Hall, 'Nulla Poena Sine Lege' (1937) Vol. 47 (2) Yale Law Journal 165-193

[30] P Darbyshire, *Darbyshire on the English Legal System* (10th edn, Sweet Maxwell 2011) 43

[31] C Elliott and F Quinn, supra, note 4, 60

[32] I Mcleod, *Legal Method*, (7th edn, Palgrave Macmillan England 2009) 267, 275; *Black-Clawson International Ltd v Papierwerke Waldhof-Aschaffenburg AG* (1975) 1 All ER 810

[33] W Tetley, 'Mixed Jurisdictions: Common Law v. Civil Law (Codified and Uncodified)' (2000) Vol. 60 (3) Louisiana Law Review 677-738

They sometimes reasoned their decision in short sentences. Accordingly, one finds very difficult to explore which type of interpretation they have used. As a result, the author has used judicial precedents from the UK and the US jurisdictions to explain how the UK and the US courts can use this type of interpretation to interpret UK and US criminal laws. For example, in *Magor and St. Mellons Rural District Council v Newport Corporation*, the purpose interpretation was used to interpret the statute. It was stated that:[34]

> We do not sit here to pull the language of Parliament to pieces and make nonsense of it ... we sit here to find out the intention of Parliament and carry it out, and we do this better by filling in the gaps and making sense of the enactment than by opening it up to destructive analyses.

The House of Lords *in Pepper v Hart*[35] confirmed the purpose approach. In this case, it was stated that:

> The days have long passed when the court adopted a strict construction view of interpretation that required them to adopt the literal meaning of the language. The courts now adopt a purposive approach, which seeks to give an effect to the true purpose of legislation, and are prepared to look at much extraneous material that bears on the background against which the legislation was enacted.

The aim of purpose approach is to discover the spirit of the legislation. If the interpretation of the statute whether it is literal or extensive explores the spirit of the legislation is called the purpose interpretation.

It might be said that the purpose interpretation may also be helpful for the Iraqi criminal judge to interpret the current theft offence laws to govern identity theft. In effect, the only real method in which the Iraqi judge may overcome the legislative inadequacy is the extensive approach. In this approach of interpretation, the Iraqi criminal judge may extend the existing theft offence laws (or create a new law) to cover identity theft. The literal approach does not allow the Iraqi judge to extend the scope of the meaning of words to encompass other words that are not stated in the statute.

Irrespective of the method that is used to interpret existing theft offence laws in Iraq, the interpretation of legislation should lead to giving the actor an idea about the

[34] *Magor and St. Mellons Rural District Council v Newport Corporation* [1952] AC 189
[35] *Pepper v Hart* (1992) 3 WLR 1032

provisions in these laws.[36] To extend existing theft offence laws the Iraqi criminal judge should examine whether the elements of theft offence can be extended to govern the elements of identity theft offence. According to literal interpretation, the judge cannot interpret the term 'property' that is mentioned in section 439 of theft offence laws to encompass a person's means of identification. He also cannot interpret the term 'appropriation' in a manner leads to extend its meaning to govern non-physical methods, such as seen, hearing or phishing that are used to obtain people's means of identification and then used it to commit other crime. However, theoretically, the Iraqi judge can use the extensive approach to extend the scope of the meaning of appropriation to encompass both physical and non-physical methods to obtain a person's means of identification. The question remains how the Iraqi criminal judge can practically use the extensive or the purpose interpretation to overcome the legislative inadequacy that is found in the current Iraqi theft offence laws. To answer this question the interpretation of theft elements will be discussed below.

5.2 To What Extent That the Iraqi Criminal Judge Can Use the Extensive Approach to Extend Theft Offence Laws

As stated previously, the extensive approach theoretically may be used to extend the scope of current laws (or to create a new law) in order to fill the gap that might be found in them. However, the question that may arise here and which needs to be answered is whether or not the Iraqi criminal judge can in practice use this approach to close the gap that has been determined previously in existing theft offence laws. To answer this question it is necessary to explore how the Iraqi criminal judge can interpret each element of theft offence and accommodate it to include the element of identity theft that corresponds to it. Nonetheless, the role of the Iraqi criminal judge may be inadequate and ineffective because the Iraqi legislation contains the principle of legality, which prevents the Iraqi judge from doing so. It is better before examining the role of the judge, illustrating the concept of the principle of legality to assess whether it constitutes a real obstacle that may prevent the judge from extending theft offence laws (or from creating new laws) to cover identity theft.

[36] K S Gallant, supra, note 5, 26; M Shahabuddeen, 'Does the Principle of Legality Stand in the Way of Progressive Development of Law?' (2004) Vol. 2 (4) Journal of International Criminal Justice 1007-1017

5.2.1 An Obstacle, Which May Prevent Judges from Plugging the Legislative Inadequacy: - 'the Principle of Legality'

The principle of legality is a tool to determine the function of powers: legislative and judicial power. It may affect the role of the judge to overcome the legislative inadequacy in the Iraqi theft offence laws to govern identity theft. It is more important to give an idea about the principle of legality below.

5.2.1.1 Definition of the Principle of Legality

The principle of legality is derived from the Latin term *nullum crimen sine lege, nulla poena sine lege* that means there is neither a crime nor punishment without a law.[37] In other words, it means that no person can be accused or punished for an act, in spite of the act being immoral or unlawful, without a pre-existing law that precisely considers this act as a crime and sets out a punishment for it.[38]

The principle of legality is applied to all types of law. However, it is frequently applied in the criminal law[39] because the criminal law includes severe penalties, such as imprisonment, the death penalty and life imprisonment, which may directly affect an individual's liberty. Consequently, most countries restrict criminal rules with the principle of legality and confine the creation of a crime and its punishment by the legislatures.

As stated above, the principle of legality consists of two elements: *nullum crimen* and *nulla peona*. There are some differences between them. For instance, *nullum crimen* protects most individuals while *nulla peona* deters criminals and affects them. *Nullum crimen* criminalises the person's conduct or shows how to punish the conduct whereas

---

[37] A Mokhtar, 'Nullum Crimen, Nulla Poena Sine Lege: Aspects and Prospects' 2005, 47 available at <http://slr.oxfordjournals.org/content/26/1/41.full.pdf> accessed on 13 August 2011, 41; P H Robinson, 'Fair Notice and Fair Adjudication Two Kinds of Legality' (2005) Vol. 154 University of Pennsylvania Law Review 335-398

[38] PH Robinson, ibid; M Shahabuddeen, supra, note 36, 1007-1017; *Landgraf v. USI Film Prods* 511 U.S. 244, 265 (1994)

[39] B Van Schaack, 'the Principle of Legality in International Criminal Law' 2009 Vol. 103 (1) American Society of International Law 101-104; RG Singer and JQ La Fond, *Examples and explanations: Criminal law* (5th edn, Aspen Publisher New York 2010) 8

nulla poena deals with the legitimacy of the real punishment or penalty itself.[40] However, both parts constitute the main body of the principle of legality.[41]

The Iraqi legislature provides the principle of legality in both the constitution and the legislation. Providing the principle of legality in the constitution and the legislation means that both the legislator and the judge must abide by the principle of legality. For example, on the one hand, the legislature cannot target or convict specific individuals without already declaring general rules in advance.[42] Additionally, the legislature cannot enact a new law and make it cover activities committed before the new law comes into force. On the other hand, the judge must also abide by the principle of legality when he/she applies the law. Therefore, Judges in courts may also refuse to apply the legislation if they believe that it is contrary to this principle.[43] However, if the principle of legality has been enshrined in the legislation only, only the judge will oblige by the principle of legality, whereas the legislature will not oblige by it.

5.2.1.2 Factors Justifying the Principle of Legality

There are many factors that may justify the existing of the principle of legality in either both constitution and legislation or in the legislation only, such as justice[44] and the protection of people.

5.2.1.2.1 Justice

Justice is a factor that may justify the existing of the principle of legality in either constitution or legislation. Justice may be achieved when the legislature, in advance, determines what the lawful and unlawful acts are. Through this determination, individuals may know which behaviour is prohibited and which is not. Then people are free to steer between these two conducts. As a result, informing people is necessary to

[40] S Dana, 'Criminal Law Beyond Retroactivity to Realizing Justice: A Theory on the Principle of Legality in International Criminal Law Sentencing' (2009) Vol. 99 (4) The Journal of Criminal Law & Criminology 857-928
[41] S Lamb, Nullum Crimen, 'Nulla Peona Sine Lege in International Criminal Law in the Rome Statute of the International Criminal Court: A Commentary' 773, 773-74, 756, (Antonia Cases, Paola Gaeta & John R. W. D. John eds., 2002) cited in ibid
[42] K S Gallant, supra, note 5, 14
[43] For example, the Supreme Court of US has invalidated legislation of constitute Military Commissions because it established contrary to applicable rules of law, *Hamdan v. Rumsfeld*, 126 S. Ct. 2749 (2006)
[44] K S Gallant, supra, note 5, 3

give them a reasonable opportunity to know what the prohibited act is.[45] The punishment also is required to be determined by a previous law and the legislature should inform people that a new Act has been enacted.[46]

Consequently, individuals will not be surprised when they are prosecuted by the courts if they commit an unlawful behaviour. Conversely, it is an injustice if a person is prosecuted for a behaviour that is not a crime under the existing law or it is a crime, but the criminals receive a punishment, which is more or less than the existing punishment. In addition, if the law or the statute has no prior notice, there may not be adequate compliance by the people accordingly the law or the statute does not accomplish its purpose to deter them.[47]

Informing people takes place when the legislature publishes the Act in the newspaper or by any other means. It is unnecessary for people to be actually informed. As a result, the Act is considered to reach the people and they are informed when it is published in media, although a small number of people, such as lawyers or scholars may read, or hear that a new Act has been enacted. Accordingly, if a person commits a crime he/she may be guilty of it.

5.2.1.2.2 Individuals' Protection

The individuals' protection is another factor, which may justify existing of the principle of legality in either constitution or legislation. The principle of legality is used as a tool to protect individuals from the legislatures or judges' arbitrariness[48] because judges under this principle are prohibited from creating a crime for an act that was committed at a time when there was no law covering it. In addition, the judge is prohibited from increasing or decreasing the existing punishment (such as fines, imprisonment and other penalties) that may be found in the existing law.

The principle of legality requires two conditions to work. The first one is the existence of laws and the second is the applicability of them. Therefore, the mere existence of a law is inadequate to protect individuals; the law should be capable of being applied.

[45] *Grayned v. City of Rockford* 92 S. Ct. 2294 (1972)
[46] *R v Chabers* [2008] EWCA Crim. 2467
[47] *Campbell v. Bennett*, 340 F. Supp. 2d 1301 (M.D. Ala. 2004)
[48] K S Gallant, supra, note 5, 3; M Jefferson, *Criminal Law* (10th edn, Pearson Education Limited Edinburgh 2011) 4; S Dana, supra, note 40

Further, the protection of individual requires that the law must not be applied retroactively[49] to cover activities committed before the law comes into force. Accordingly, the law should immediately be applied to cover act(s) that may happen after it has come into force, and it should not be applied to cover act(s) that happened before this time. In addition, statutes should be published in order to inform individuals what the unlawful or lawful act is.[50]

After this brief preamble of the principle of legality, it is important to clarify the role of the judge to scrutinise and to examine whether he can extend these laws according to above rules (or create new laws) to overcome the inadequacy that is found in them, or that prevents the application of these laws to cover identity theft.

5.2.2 The Role of the Iraqi Criminal Judge to Fill in the Gap in the Current Theft Offence Laws

As stated previously, two methods may be used to close the gap in existing theft offence laws: Widely interpreting the current theft offence laws and the analogy.

5.2.2.1 Closing the Gap by Widely Interpreting the Current Theft Offence Laws

As noted previously, the judge can interpret an ambiguous and unclear statute to explore the spirit of it. In some legislation, the judge can also widely interpret the statute to fill in the gap that may be found in the legislation. In this section, the way that may be used to answer the question, which has previously been risen and needs to be answered, whether the Iraqi criminal judge can widely interpret existing theft offence laws to govern identity theft, will be discussed below.

The role of the Iraqi judge to extend existing theft offence laws (or to create a new law) by interpreting them can be examined through the courts' decisions. These decisions may assist the author to analyse the elements of theft to scrutinise whether the criminal judge can interpret them and extend the scope of their meaning to cover identity theft. There are two types of criminal courts in Iraq, which deal with the interpretation of statutes: the lower courts and the higher courts. Judges in higher courts and the lower

[49] K S Gallant, supra, note, 5, 3

[50] *Bynum v. State*, 767 S.W.2d 769, 773 (Tex. Crim. App. 1989); *State of Texas v River Forest Development Co.* 315 S.W. 3d 128 (Tex. App. Houston [1 Dist.] 2010

courts interpret the ambiguous statute to determine its meaning to apply it to a person who commits unlawful acts.[51] Higher court's decisions only can be as precedent cases that in which the author can examine the role of the Iraqi judge to extend existing theft offence laws to govern identity theft.

The judges of the higher court may decide many decisions after they discuss cases that have been ruled by the judges in lower courts, and then appealed before them. In The higher court, for example, the lower court's decision may be confirmed if the lower court's decision was in accordance with the law.[52] Alternatively, it may be overruled by the higher court and the case is returned to the lower court if the higher court notices that there is a mistake in the interpretation of the statute.[53]

On the other hands, judges of the higher court may acquit the accused if they or most of them noticed that there is no evidence or that the evidence is inadequate to judge the accused.[54] They or most of them may also increase or decrease the punishment if they are persuaded that the punishment is disproportionate to the seriousness or not of the crime that is committed.[55] However, the increasing or decreasing of punishment will be

[51] *A and Others v. Criminal Centre Court* Integrity Commission Court of Appeal Public Commission [2007] 42. In this case, the court of appeal tried to construe section 1/7 that was issued by the occupied power in 2004. Section 1/7 stated that the authority of council commissioners of Electoral Integrity Commission has authority to send any criminal case to the authorities if it finds evidence about criminal behaviour relates to integrity process of elections. According to this section, the council is the sole reference that its permission should be taken before accusing any member of the Integrity commission who commits a crime relates to integrity commission process and sending him to the court. The court of appeals interpreted section 1/7 and found that this section confers obtaining permission from the council with respect to the crimes that are committed and related to the integrity elections process only. The ordinary crimes that are committed beyond the integrity elections process need no permission to accuse the member or send him to the court. The court reasoned its decision that the case does not relate to integrity of elections process and there is no legal text that needs taking permission to send the accused to the court. In addition, the Integrity Commission is considered independent Commission and it obeys to Parliament. Moreover, its members do not consider professionals in any government institutions and section 1/7 that has regulated and governed it did not refer to get permission in order to send the accused who commits a crime, which is not related to the integrity of elections process. Therefore, there is no necessary to take permission to send the accused to the court if he commits ordinary crime.

[52] *M v. Criminal Central Court of Karbala* Iraqi Court of Cassation Expanded Commission [2009] 154; *J* and *Others v. Delinquents Court of Wasit* Iraqi Court of Cassation Extended Commission [2006] 55

[53] *S and Others v. Criminal Central Court of Baghdad* Iraqi Court of Cassation Public Commission [2007] 19

[54] *Prosecutor v. Criminal Court of Basra* Iraqi Court of Cassation Second Criminal Commission [2010] 2018, 2019

[55] *K and Others v. Criminal Central Court of Mesan*, Iraqi Court of Cassation, Public Commission, [2010] 91. The Court of Cassation found that there were some circumstances required increase the punishment. Therefore, it increased the punishment to capital penal. However, the victim waived his right to punish the accused. Consequently, the Court of Cassation decreased the punishment to imprisonment 20 years.

determined within the scope of the original punishment that is formulated by the legislature.

If judges or most of them in the higher court or the lower court believe that, there is a certain degree of vagueness in the statute, they may reject the application of the vague statute on the grounds of unconstitutionality, but they cannot abolish it. There are many circumstances which may cause vagueness in the statute, such as where the definition of the crime is inadequate,[56] where there is vagueness which may affect the deterrent purpose of the legislation,[57] or where the legislature does not give people fair warning about one or more of elements of a crime.[58]

Judges of the Higher Court cannot abolish the unconstitutional laws because abolishing a law is the legislatures' function according to the principle of legality. If the judges of the Higher Court abolished the unconstitutional laws, they may usurp the legislature's function and violate the principle of legality.[59] The only thing that judges in higher court can do is they may require the legislature to abolish the unconstitutional statute. In same vein, the House of Lords in *R v Jones and Others*[60] stated that the statute law that is created by Parliament is the main source of new crimes. It also clearly stated that judges had no right to create a new crime in the area of criminal law. Moreover, it stated that the judges cannot abolish crimes, but they have a right to overrule cases, which are inconsistent with Article 7 of the European Convention on Human Rights.

From the above discussion, it seems that Iraqi criminal judges cannot extend theft offence laws (or creating new laws) to govern identity theft. However, extending theft offence laws may not be impossible, particularly legislation sometimes is ambiguous, or the legislature occasionally formulates the law in a way that may allow the judge to interpret it expansively to encompass unpredictable unlawful activities. Some unlawful activities may be unpredicted by legislatures when they enact a specific law to govern predicted unlawful activities, thus, these unpredictable unlawful activities may not be

[56] *Kolender v. Lawson* 461 U.S. 352, 357 (1983)
[57] *Cuevas v. Royal D'Iberville Hotel* 498 So. 2d 346, 358 (Miss. 1986)
[58] *Vill. of Hoffman Estates v. Flipside Hoffman Estates Inc.* 455 U.S. 489, 499 (1982)
[59] Interview with Dr. A Baaj, Specialist in criminal law and a lecturer at Baghdad University School of Law (Baghdad, 30 January 2013); M Abdul Ali, Deputy President of Federal Court of Appeal of Baghdad Rusafa, Presidency of Appeal Baghdad Federal Court (Baghdad, 27 January 2013)
[60] (2006) 2 WLR 772

subject to this new law. Consequently, judges can extend the law to encompass them. For instance, although the recent tendency believes that the UK judge cannot create a crime or set out a punishment for it. However, the House of Lords in *R v C* has created the law.[61] In this case, the House of Lords has abolished long-standing immunity and convicted in 2003 a husband who raped his wife in 1970 and who had been acquitted because his conduct was not a crime at that time.

Accordingly, one may assume that the Iraqi judge cannot wait until the Iraqi legislature amends the current theft offence laws (or creates new laws) to overcome the inadequacy of these laws. Judges should interpret these laws to cover identity theft until the new law is being enacted. By doing so, the judge should interpret the elements of theft offence to extend the scope of their meaning to include the elements of identity theft. As stated previously, identity theft consists of two main elements *actus reus*, *mens rea* and a specific third element is the subject matter that is represented by the means of identification. These elements differ from the elements of conventional theft that are stated in the current theft offence laws in Iraq.

Judges in some jurisdiction can overcome such inadequacy in their legislation by expanding the current laws to cover the illegal activity. It was noticed that judge could use the extensive interpretation or analogy to expand the law. The analogy as a means to expand (or to create a new law) will be discussed later. To expand existing theft offence laws the Iraqi judge should interpret each element of theft offence to examine whether it can be expanded to govern the element of identity theft that corresponds to it or not. The first element that the judge should start with is the appropriation.

5.2.2.1.1 Interpreting the Term Appropriation

Appropriation is the key that can be used to examine whether the Iraqi judge can interpret and extend the scope of theft offence laws to cover identity theft. The Iraqi judge may interpret the term ‘appropriation’ and extend its scope to meet the obtaining of a person’s means of identification or what is called the *actus reus* of identity theft. As stated previously, in existing theft offence laws, the Iraqi legislature does not define

[61] [2004] EWCA Crim 292; *R v Dica* [2004] EWCA Crim 1103 [2004] QB 1257

this element.[62] Therefore, jurisprudence has defined it. It has been defined as any physical activity that is conducted by the accused to appropriate another person's property and appear as its own.[63] The lack in the definition of the *term appropriation* may present an opportunity to the Iraqi criminal judge to interpret it and determine what the actual meaning of the term 'appropriation' is. The author has not found decisions from Iraqi judges to support his argument about how the Iraqi judge can extend the meaning of appropriation to accommodate it to cover the *actus reus* of identity theft. Therefore, he resorts to the US and the UK precedents to support his argument.

To explore the meaning of the term 'appropriation', the judge should seek the meaning of it in the structure of the text, language dictionaries, the history of theft offence laws, and the purpose of the law. From the background of the discussion of these laws within government and Parliament, the judge can decide whether the Iraqi legislature intended when it used the term appropriation in theft offence laws as an element of theft to include both physical and non-physical methods to commit theft offence.[64] If the judge explores that the term appropriation means both physical and non-physical methods he can use it as *actus reus* of identity theft. The judge can rule a person who lawfully or unlawfully obtains another person's means of identification with intent to commit other crime because non-physical methods constitute the *actus reus* of identity theft. Identity theft takes place when the accused copy, sees or hears another person's means of identification and then memorises it to use it to commit other crimes. Copying, seeing or hearing is a non-physical method and it constitutes the *actus reus* of identity theft.

However, the Iraqi judge is reluctant to interpret theft offence laws and expand the meaning of the term 'appropriation' to govern the copying, seeing or hearing as an

---

[62] See chapter four of this thesis

[63] S Atallah, 'The Actus Reus of Theft' 2011, 1 available at <http://www.shaimaaatalla.com/vb/showthread.php?t=9963> accessed on 9 March 2013

[64] *Dred Scott v. Sandford*, 60 U.S. 393, 19 How 393, (1857) Supreme Court of United States, the court stated that '[i]n the opinion of the court, the legislation and histories of the times, and the language used in the Declaration of Independence, show, that neither the class of persons who had been imported as slaves, nor their descendants, whether they had become free or not, were then acknowledged as a part of the people, nor intended to be included in the general words used in that memorable instrument'; *Pepper v Hart* [1993] AC 593, in this case, it was stated that '[t]he days have long passed when the courts adopted a strict constructionist view of interpretation, which required them to adopt the literal meaning of the language. The courts now adopt a purposive approach, which seeks to give effect to the true purpose of legislation and are prepared to look at much extraneous material that bears upon the background against which the legislation was enacted'; *United Stated v. Lyons* 706 F.2d 321 (5th Cir.1984); *United States v. Neapolitan*, 791 F.2d 489 (7th Cir. 1986)

element of identity theft because he believes that by expanding the scope of the meaning of the term appropriation he may violate the principle of legality. The whole thing that the Iraqi judge can do is interpreting the statute in a manner that does not lead to offend the principle of legality and create a new crime. In *Duty Prosecutor and A v. Hilla Court of Misdemeanours*,[65] for instance, the judge has extensively interpreted and extended the *actus reus* of the offence of breaking the house to encompass the non-physical entrance. The legislature in section 428 (1) states that a person is guilty of house breaking if S/he enters a house, part of it or, parts belongs to that house without permission.

Given the above incident, the Iraqi legislature does not determine whether the entry into the house should be either physical or nonphysical. Consequently, Hilla court has extensively interpreted the statute. The Hilla court stated that the accused is guilty of house breaking and entry as well as infringed his private life. The court's ruling relied on the ambiguity of the legislation as well as intruding into another person's private life. This act is sanctioned in Iraq's law. Thus, in this context, the court had extended the scope of the *actus reus* beyond house breaking and unlawful entry to include moral values, such as intruding into individual's private life. Upon appealing, the lower court's decision was confirmed by the Federal Court of Appeal of Babylon.

The aforementioned decision has been criticised by another Iraqi judge.[66] This judge stated that although the Iraqi judge is prohibited by section 19 (4) of the Iraqi Penal Code 1969 from using analogy to create a new law the judge at the Federal Court of Appeal of Babylon, in the above case, has used the analogy in criminal law and created a new crime and set out a punishment. It could be said that the judge of Babylon Appeal has not used the analogy because the analogy as will be shown completely different of what the court decided. The court in this case has widely interpreted and extended the scope of section 1of the article 428 to include also non-physical entrance.

---

[65] Federal Court of Appeal of Babylon T/J/ 30/10/2012, 455, 456 in this case, the court did not interpret an ambiguous law. As the court stated, the law was unambiguous, however, it was deliberately and extraordinary abroad. Consequently, the court was persuaded by conditions of the agreement for conspiracy and the punishment. It relied on precedent cases of others circuit courts and statutes that deal with the same issue.

[66] S. Al Musawi, 'The Analogy in Criminal Law (Comment on the Decision of Federal Court of Appeal of Babylon as Court of Cassation) Modern Argument' No. 3907, 10/11/2012 available at <http://www.ahewar.org/debat/show.art.asp?aid=331863> accessed on 10 March 2013

The Iraqi judge can interpret the term appropriation as an element of theft offence to distinguish between crimes only. In other words, he interprets it to examine whether an illegal act constitutes an element of theft or it constitutes an element of another crime, such as fraud or betrayal trust.[67] It is import here to state that all the higher court decisions fall within the scope of law. In other words, judges of the higher court take these decisions according to the discretion that the law grants it to them.

The question that may appear and one may not find an answer for it as to why the Iraqi judge is reluctant to interpret the term appropriation and extend the scope of their meaning. While in the US, the legislation sometimes may also be ambiguous, but judges in US courts, when they encounter any ambiguous or lack in the legislation they are not reluctant to interpret the statute and widely interpret it to explore a solution for the lack that may appear in the US legislation. When the US courts attempt to interpret the ambiguous legislation they may look for the solution in language dictionaries, circumstances that surround the enactment of the legislation or the history of legislation to infer the intention of the legislature that it intended when it enacted the statute.

In the Computer Fraud and Abuse Act 1984, for instance, the US legislature has not defined the term of 'without authorised', which makes the Act ambiguous. As a result, judges in the US courts have attempted to solve and clarify the ambiguity of this Act. In *United States v. Ivanov*,[68] the court stated that the term 'without authority' means a person lack authority to access another person's computer. This interpreting of the statute is easy because the ambiguous is not huge and the judge can easily remove it. However, in some cases it is difficult to determine whether the access with or without authority, particularly if the criminal has some authority to access individuals' computers. The majority of US courts whether civil or criminal courts held that without authority occurs if and only when the criminal has no permission to use the computer

[67] *A v. Criminal Central Court of Mesan*, Iraqi Court of Cassation, Criminal Commission [2006] 6178. In this case, the accused was responsible to protect the election's centre. When he saw the people had crowded at the election's centre, he fired a bullet at people. By this act, he killed a one person and injured the other. The court ruled the accused on manslaughter. Due to the Court of Cassation has authority on all lower courts decisions, it requested the case papers because it noticed that there was violation in law application. After it had carefully studied the case papers, it decided changing the type of a crime. It stated that the crime that happened was murder not manslaughter; *F v. Criminal Court of Rusafa* Iraqi Court of Cassation Extended Criminal Commission [2011]. In this case, the Court of Cassation also changed the type of a crime from murder to self-defence. As a result, the Court of Cassation acquitted the accused.

[68] *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001)

for any purpose.[69]

In addition, in other cases, judges in the US's courts extensively interpreted the coercion as an element of a human traffic crime that set forth in Traffic Victim Protection Act of 2000 and extended the scope of its meaning to encompass non-physical coercion. In *United States v. Kozminksi*,[70] for instance, the court held that coercion did not limited to physical and legal coercion; however, it also includes psychological coercion.

In the same context, in the UK, the House of Lords in *R v Clegg*[71] broadly interpreted the statute. It considered the accused's act as a crime whereas he committed this act according to his duty. However, according to criminal law committing a crime whilst on duty or during enforcement of the law is not a crime.[72] The facts in this case were that the perpetrator was a soldier on a duty to catch fugitives. During his duty a car passed by at speed. There was no indication that it would stop, so he shot at the front side of the windscreen. When the car passed, he fired another bullet at the rear side of the car and killed a passenger. The House of Lords considered the soldier's act as murder and not as self-defence.

Furthermore, although the jurisprudence in UK define the assault that constitutes the *actus reus* of battery as an act, which requests physical movement to cause a apprehension of harm,[73] two courts in UK have widely interpreted the *actus reus* of 'assault' to encompass non-physical act as well. For example, the Appeal Court in the *Ireland*[74] stated that the accused was guilty of assault because he terrified another person by words, while battery was defined as a physical act. The UK judge also in the *Fagan*[75] case defined 'an assault' as 'any act which intentionally or possibly recklessly causes another person to apprehend immediate and unlawful violence.'

---

[69] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133-34 (9th Cir. 2009); *B&B Microscopes v. Armogida*, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007)

[70] *United States v. Kozminksi* 487 U.S. 931 (1988); in *Catalan v. Vermillion Ranch Ltd.*, the court expanded the *actus reus* of threating crime to encompass physical to verbal threats of abusing the legal process No. 06-cv-01043-WYD-MJW, 2007 U.S. Dist. LEXIS 567, at *23-24 (D. Colo. Jan. 4, 2007); *States v. Veerapol*, 312 F.3d 1128, 1132 (9th Cir. 2007)

[71] [1995] 2 WLR 80

[72] Section 3 (1) Criminal Law 1967 c, 58 (UK)

[73] D Ormerod, *Smith and Hogan, Criminal law* (12th edn, OUP Oxford 2008) 584

[74] *R v Ireland* [1998] AC 147

[75] *Fagan v Commissioner of Metropolitan Police* (1969) 1QB 439

It could be said that interpreting the term of appropriation, which is stated in the current theft laws in Iraq is necessary; particularly the Iraqi legislature has not defined it. The definition of appropriation has become as matter of judges and jurisprudence interpretation. Both judges and scholars can interpret the term 'appropriation' to explore its meaning and determine its scope. Interpreting existing theft offence laws does not violate the principle of legality that is provided in the Iraqi Penal Code because the principle of legality aims to achieve the justice and protect people from illegal activities. Consequently, the justice and people's protection may be achieved when their means of identification is protected from the act of the illegal obtaining of people's means of identification, and then using to commit other crimes in their names. The history of theft offence laws and language dictionaries has not limited the term 'appropriation' to physical action only. The author believes that the term appropriation, which is set out in theft offence laws, includes both physical and non-physical methods that may be used by people to commit a crime. Accordingly, the *actus reus* of identity theft falls within the scope of the conventional theft offence.

However, if it is summed that the Iraqi criminal judge can extensively interpret the *actus reus* (the term appropriation) of theft and accommodate it to meet the *actus reus* (appropriation or the act of the unlawful obtaining of a person's means of identification) of identity theft, another obstacle may appear. This obstacle is can the *mens rea* of the traditional theft offence be openly interpreted and accommodated to meet the *mens rea* of identity theft.

5.2.2.1.2 Interpreting *Mens Rea* of Theft Offence

In existing theft offence laws, the Iraqi legislature also does not define the element of *mens rea* of theft. By doing so, it has presented another opportunity to the Iraqi judge to extend the current theft offence laws by interpreting the *mens rea* of theft offence to extend the scope of its meaning to encompass the *mens rea* of identity theft. In the current theft offence laws, the legislature has stated the term 'intentionally' only. The term intentionally refers to that the accused knows the elements of crimes, such as theft offences that he commits them only. For instance, the accused knows that he takes another person's movable property without his consent. However, this is not enough to determine whether taking another person's movable property for a period of time

constitutes theft. The Iraqi judge does not need to interpret the terms 'knowingly or intentionally' because most crimes that are committed against people's properties are considered intentional crimes. Nevertheless, as it happened with US courts, the terms 'knowingly or intentionally' may sometimes give rise to an issue whether these terms describe the verb or the object, and this issue may trigger the ambiguity of legislation. US courts have presented an intensive analysis to this issue, particularly the analysis that dealt with the term knowingly, which has been stated as an element of aggravate identity theft stated in the Identity Theft Penalty Enhancement Act of 2004.[76]

The Iraqi legislature does not determine whether theft is committed by taking another person's property permanently or temporarily. Contrary to most jurisdictions and particularly the US and UK jurisdictions, which have been chosen as a reference in this study expressly state that a person is guilty of theft if he with an intent to permanently deprive the owner appropriates another person's property.[77] The Iraqi legislature has not stated that theft must be committed with an intention to permanently deprive the owner of his property as an element of theft.

It might be said that the omission of the term 'an intention to permanently deprive the owner of his property' as an element of *mens rea* of theft makes theft offence laws in this point ambiguous. This ambiguity in the definition of the *mens rea* raises difficulties when theft offence laws are applied to identity theft.[78] According to the Iraqi Penal

[76] *United States v. Pebworth*, 112 F.3d 168, 171 (4th Cir. 1998); *United States v. Mendoza-Gonzalez*, 520 F.3d 912, 915 (8th Cir. 2008); *United States v. Hurtado*, 508 F.3d 603, 607 (11th Cir. 2007) cert. denied, ---- U.S. ----, 128 S.Ct. 2903, 171 L.Ed.2d 843 (2008); *United States v. Montejo*, 442 F.3d 213, 214 (4th Cir. 2006) cert. denied, 549 U.S. 879, 127 S.Ct. 366, 166 L.Ed.2d 138

[77] Section 223.2(1) of the Model Penal Code 192; section 6(1)Theft Act 1968 (UK)

[78] In this footnote, the author states some cases to prove that the statute should not be ambiguous. As well, he presents the way that were used by US courts to resolve the ambiguity of the statute, for instance, in *United States of America v. Satelo* the court pointed out that section 1028A (a) (1) is ambiguous. The legislature does not determine that the term knowingly that is required in aggravated identity theft encompass both the verb and the object, thus, the government should prove that the accused knows when uses a means of identification it belongs to another person. The court relied on the purpose, legislation history and its language to interpret section (1028), United States Court of Appeals 515 F.3d 1234, 380 U.S.App.D.C. 11; in *United States v. Godin*, the court stated that '[t]he question before this court is how far the 'knowingly' *mens rea* requirement extends. Must the defendant know that the means of identification belongs to another person? We conclude that the statute is ambiguous and that the legislative history does not clearly reveal congressional intent. Applying the rule of lenity, as we must, we hold that the 'knowingly' *mens rea* requirement extends to "of another person." In other words, to obtain a conviction under § 1028A (a) (1), the government must prove that the defendant knew that the means of identification transferred, possessed, or used during the commission of an enumerated felony belonged to another person", 476 F. Supp. 2d 1, 2 (D. Me. 2007) U.S. 879, 127 S.Ct. 366, 166 L.Ed.2d 138 (2006)

Code 1969, there is no dispute that either theft or identity theft if it is considered as a crime is an intentional crime. They cannot be committed by recklessness or negligence. The difficulty may arise when the accused takes another person's property temporarily. He has an intention to return it after the use of it. Does this case constitute theft according to the current Iraqi theft offence laws?

Most scholars and judges believe that the theft offence takes place only when the criminal knowingly and intentionally takes another person's property with intent to permanently deprive him of it, even if the Iraqi legislature does not state the term 'intent to permanently deprive the owner' in the current theft offence laws. They also believe that there is no theft when the criminal takes another person's property to use it for period of time and then returns it. According to this opinion, the act of the unlawful obtaining of another person's means of identity theft does not fall within the scope of theft and the current theft offence laws cannot be applied to this type of crime. However, it could be argued that existing theft offence laws are also ambiguous in this point. The scholars and judges' belief should not prevent the Iraqi criminal judge from interpreting the definition of *mens rea* and from expanding the scope of its meaning in a manner that governs the state of mind of the accused when he obtains another person's means of identification with intent to commit other crimes.

Iraqi judges should not be reluctant to interpret theft offence laws to explore the spirit of theft offence laws and to remove their ambiguity. There are many reasons that may justify the interpretation of *mens rea* of theft offence and extending the scope of its meaning to include the *mens rea* of identity theft. Firstly, the Iraqi legislature does not precisely define the *mens rea* of the traditional theft offence. Secondly, as mentioned previously and contrary to UK jurisdiction, the interpreting of existing theft offence laws by the Iraqi judge does not oblige the lower judge or the judge in same level. The judicial interpretation also does not oblige even the judge himself. As a result, the Iraqi judge can leave the interpretation that he has adopted in a previous case and adopt a new one in the same case or in another case when it comes before him.

Theoretically, the Iraqi criminal judge can interpret the *mens rea* of theft offence and expand its scope to cover the *mens rea* of identity theft offence, but in practice, Iraqi criminal judges are reluctant from doing so. They think that if they interpret theft

offence laws and extend their scope to include the *mens rea* of identity theft or any other elements of identity theft they may create a new crime. If the judge creates a new crime, he may violate the principle of legality, which prevents judges from creating a crime and setting out a punishment for it.[79] For example, the Iraqi Court of Cassation in *S and others v. Criminal Court of Baghdad* overruled a decision that was taken by Criminal Court of Baghdad.[80] In this case, the criminal court of Baghdad decided that the accused's act constitutes three crimes not one crime. However, the Court of Cassation stated that the Criminal Court made a mistake in statute interpretation because the incident that was committed if it had been proved constitutes a one crime not three crimes.

In addition, the Iraqi judge Contrary to the UK judge has not been empowered to create a new crime and set out a punishment for it. Consequently, the Iraqi criminal judge cannot widely interpret theft offence laws to govern identity, whereas the UK judge can widely interpret existing theft laws or any other laws to cover identity theft.

It might be said that the principle of legality should not stand an obstacle, preventing Iraqi judges from extending theft offence laws to govern identity theft if there is a way to extend these laws. For instance, in the US jurisdiction, which is taken as a reference to compare with Iraqi jurisdiction, although the US has adopted the principle of legality in their legislation, US judges can widely interpret existing laws and expand the scope of them to cover illegal activities.

In the US there are no decisions from the US court refer to interpreting theft offence laws to apply them to identity theft because as it will be shown in the next chapter, the US has two laws that deal with identity theft. However, the US judges have, contrary to general rules of interpretation, broadly interpreted these identity theft laws and extend

[79] *S v. Criminal Central Court of Baghdad* Iraqi Court of Cassation Public Commission [2008] 282, in this case, the court of appeal requested the papers of the case. After it has discussed these papers, it overruled the decision that was issued by Criminal Court of Baghdad. The court of appeal acquitted the accused because his crime was repealed by a decision was issued by the Commission of Amnesty and the court of Baghdad made a mistake in the law application when it judged the accused on a repealed crime.

[80] *S and Others v. Criminal Central Court of Baghdad* Iraqi Court of Cassation Public Commission [2007] 19; the Iraqi Court of Cassation in *A v. Criminal Court of Babylon* also overruled a decision was issued by Criminal Court of Babylon. The Court of Cassation pointed out that the Criminal Court made a mistake when it appreciated the evidence that were mentioned. Iraqi Court of Cassation Public Commission [2007] 79; *A v. Criminal Court of Diywania*, Iraqi Court of Cassation, Public Commission, [2006] 158; *A v. K* Court of Cassation [1971] 177 the court stated that the bar could not be considered as a bank, shop or a storage because theft offence laws did not stated it as a bank.

their scope to encompass even the use of people's identities with their consent to commit other crimes.

With respect to how judges can widely interpret the ambiguous statutes that relate to the *mens rea* of the crime to fill in the gap that may be found in them, the study attempts to state some decisions to examine how the US judges can interpret their ambiguous laws and then expand their scope to fill in the gap that may be found in the legislation. For instance, in *Shurgard Storage Centers,Inc. v. Safeguard Self Storage, Inc.,*[81] the court construe the term 'intent to defraud' that has been stated in section 130 (a) (4) of the Computer Fraud and Abuse Act. The court stated that the term 'intent to defraud' refers to 'wrongdoing' and it does not need providing the elements of the common law elements of fraud. In the same vein, the court of sixth circuit extensively interpreted the unlawful act that has been stated in section 511 (2) (d) and expanded the scope of it to cover recoding surreptitiously a conversation of party who already has given his consent to participate in the conversation.

> Our court, in Cincinnati Post & Times-Star, considered itself bound by the prior determination that the recording was not illegal. However, the language and legislative history of the statute clearly demonstrate that the privilege is not extended if the intercepting party acted with the purpose of committing a criminal, tortious, or injurious act.

In another case, the US Supreme Court Sentences interpreted an ambiguous statute to favour of the accused. In *Ratlaf v. United States,* the Supreme Court tried to interpret the terms "willfully violating" that is stated in section 5322, to apply it to section 5324. It pointed out that section 5324 requires convicting the defendant proof that the defendant knew not only of the bank's duty to report cash transactions in excess of $10,000, but also of his duty not to avoid triggering such a report. However, the term 'willfulness' that is stated in section 5322 is ambiguous and could not be applied to section 5324. The court stated that there is contrary indication in the statute's history, thus, to solve such ambiguous in legislation the legislation should be interpreted in favour of the accused.[82]

---

[81] *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000)

[82] *Ratlaf v. United States*, Certiorari to the United States Court of Appeals, No. 92-1196, (9th Cir. 1994); *Ratzlaf v. United States* 507 U.S. 1050, 113 S. Ct. 1942 (Mem) U.S. 1993

It could be said that although the US legislature has adopted the principle of legality in their legislation, the US criminal judges, however, interpreted the ambiguous laws and expanded their scope to cover the means that was not expressly stated in law and used to commit a crime. As a result, it might be argued that there is no an obstacle to prevent an Iraqi judge to interpret the *mens rea* of theft and expand the scope of it to cover the *mens rea* of identity theft particularly, the Iraqi legislature does not precisely define the *mens rea* of theft. If the judge interprets theft offence laws and extends the scope of its meaning to meet the *mens rea* of identity theft, he does not violate the principle of legality because the Iraqi legislature does not mention that theft takes place when the criminal takes another person's property with intention of permanently depriving him of it. Consequently, theft is committed and the accused may be guilty of theft, even if he uses another person's property temporary. By doing so, the criminal judge does not create a new crime, as well as he does not offend the principle of legality.

According to the above analysis or the author's conclusion, the Iraqi judge can extend both the *actus reus* and *mens rea* of the Iraqi traditional theft offence to meet the *actus reus* and *mens rea* of identity theft. However, A question remains is can the Iraqi criminal judge interpret the term 'property' that is stated in section 439 of the current Iraqi theft offence laws to be adequate to cover another person's means of identification as a type of it.

5.2.2.1.3 Interpreting Theft Offence Laws to Extend the Meaning of Property

Section 439 of existing Iraqi theft offence laws states that if property is to be subject to theft it should be a movable and tangible thing. According to this section, two conditions should be available in property to be a subject of theft: movable and tangible. Movable generally denotes that something can be moved from one place to another; while tangible means that something can be touched and cognizable or it is a thing that is capable of being touched; discernible by touch[83]; material or substantial.

If the thing is not movable and tangible, it cannot be subject to theft. Literally, a person's means of identification is not subject to theft because it is intangible and

[83] Team of Hiregange- Bangalore and Hyderabad, 'What is the Service Tax, Service Tax Concepts Updated Upto 01. 10. 2012' 2012, 226 available at <www.simpletaxindia.net> accessed on 22 January, 2014

cannot be moved from one place to another. It is a non-cognizable thing. By providing these two conditions of property as subject to theft in the current theft offence laws, these laws become unambiguous and do not require interpretation. According to the two conditions of property that are provided by the Iraqi legislature, the Iraqi criminal judge has no an opportunity to interpret the term 'property' expansively and to extend the scope of its meaning to govern a person's means of identification. According to the principles of interpretation of statues, the judge can only interpret the statute when there is ambiguous in it. However, existing Iraqi theft offences laws that relate to the term 'property' as subject to theft are clear and unambiguous. Consequently, if the Iraqi criminal judge expansively interprets the term property to cover the means of identification to be subject to theft, he may violate the principle of legality.

One may assume that the Iraqi judge may not violate the principle of legality if he widely interprets the current theft offence laws to explore the spirit of them only, even if the interpretation leads to creating a new crime. Particularly, the legislation cannot keep pace with the technological development. In addition, enacting a new law by parliament takes a long time and during this period of time, many identities can be stolen, and then used to commit other crimes. People may also lose their money and the economy of the state may be wrecked. Consequently, the judge needs to interpret the term 'property' that set forth in the current Iraqi theft offence laws expansively to cover people's means of identification. The aim is the same whether the Iraqi legislature enacts law to protect people's tangible properties or to protect their intangible things. The aim of theft offence laws is protecting people's owns and deterring other unscrupulous persons to obtain people's properties, such as their cars, money or any other properties.

For instance, when the criminal steals another person's movable property, he directly uses it and exhausts its value. Whereas in case of the act of the unlawful obtaining of another person's intangible thing, such as his means of identification he uses the stolen identity to exhaust the value of his other properties, such as his money or to ruin his reputation. Crimes, which are committed by using another person's means of identification, may cause vast damage to the victim. The damage that caused by using stolen identity of another person may be much than the damage that is caused by stealing the tangible movable property of another person because the criminal may

continue to use the victim's means of identification until he dries the victim's account. The motive to protect a person's means of identification is more important than the motive required to protect their tangible properties; especially this means has become an indispensable tool in people's transactions either offline or online.

In addition, with internet emergence, for instance, the faceless transactions have increased; therefore, unscrupulous persons seek to obtain people's means of identification in any way to accomplish their illegal ends. If the Iraqi criminal judge takes into account the above justifications and expansively interprets existing theft offence laws, he will prevent people from being a victim of identity theft and achieve the justice that both Iraqi theft offence laws and the principle of legality aim to achieve it.

However, it may be impossible to adopt a hypothesis like the aforementioned hypothesis because the principle of legality also aims to protect people to being subject to criminal liability before they are informed by the legislature or judges that an act has become a crime. Main consequences of the principle of legality are preventing the legislator from enacting a new law to be applied retroactivity and preventing the judge from applying the law retroactivity. People should be informed that a new act has been enacted. As the judge Almusawi[84] stated in his article named 'the definition of a terrorism crime', the Iraqi judge could not brand an illegal activity as a crime unless he finds a legal text that criminalises it. Otherwise, he should acquit the accused. He also stated that the Iraqi legislature should enact a new act, as it did in 2005 when it enacted the Terrorist Act 13 of 2005, to overcome the inadequacy *of the current theft offence laws* that is determined by judges.

Another issue may prevent Iraqi judges to adopt the above hypothesis, which is the Iraqi society either commonalty or specialists, such as scholars or judges cannot accept this hypothesis because they have no knowledge about modern crimes and how they can be encountered. They still adhere to traditional provisions that punish a person who steals another person's car or abducts him. They are far from technology and they live in yesterday. However, the aforementioned hypothesis can be workable if one takes into

[84] S Al Musawi, 'The Definition of Terrorist Crime', Shabaka al Nabaa News 29/11/2008, available at <http://www.annabaa.org/nbanews/72/067.htm> accessed on 12 March 2013

account the opinion, that the criminal by his immoral taking of another person's means of identification, sacrifices his right to be informed that a new law has been enacted.

From the previous analysis of the elements of theft, it might be argued that the Iraqi criminal judge cannot extend the scope of the current theft offence laws, which were enacted particularly to deal with a moveable corporeal property only, to cover the legal or illegal obtaining of another person's means of identification, and then using to commit other crimes. In addition, the Iraqi criminal judge cannot create a new law to govern this type of crime and set a punishment for it, even if there are strong reasons to create a new crime and set a punishment for it because criminal judges in Iraq oblige by the principle of legality. This principle grants the legislature only as a power to creating the law, and prevents the judges from creating a new crime or setting out a punishment in circumstances where they do not find a rule that covers the unlawful act, such as the act of the unlawful obtaining of another person's means of identification.

It could also be said that not just the Iraqi criminal judge cannot expand existing theft offence laws; even the UK and US judges currently cannot interpret their existing theft offence laws in a manner that may govern identity theft (or create news laws) to govern it. Consequently, the author believes that the judicial framework of both the UK and US represented by the case law created by judges cannot effectively be used to assist Iraqi judges to fill in the gap in the current Iraqi theft offence laws.

The question remains is if the Iraqi criminal judge had no power to extend the scope of existing theft offence laws by interpreting them, (or create new laws) to govern identity theft can he use the means of analogy to find a solution and fill the gap in the current Iraqi theft offence laws. In other words, can the judge search in the whole criminal law to explore a rule that deals with the manipulation or misuse of an intangible property and apply it to identity theft. This issue will be discussed in further detail in the next section.

5.2.2.2 The Role of the Iraqi Judge to Overcome the Inadequacy in Existing Theft Offence Laws by Analogy

As mentioned previously, judges in most countries can fill in the gaps that may appear in their legislation by either interpreting existing laws and extend their scope to govern

the new illegal activities, or by using the analogy to criminalise these illegal activities. Iraqi judges are some of those judges who may close the gap that was determined in existing theft offence laws by using the analogy. Therefore, the analogy as a means to fill in the gap will be discussed below.

5.2.2.2.1 Analogy

Analogy means criminalising an illegal act that has not been sat out in the current criminal law by measuring it on a similar act that has been criminalised by the current criminal law because the two acts involved have similar elements.[85] By analogy, some acts that are actually outside the coverage of the criminal statute are also considered as crimes because they have some elements of the acts that are covered by the existing criminal law.[86] For instance, if there are no provisions in the current statute to cover the illegal act that takes place, but there are provisions covering another unlawful act that is similar to the first act in most of its elements,[87] the first act may be covered by the provisions that cover the second act by analogy.

If the aforementioned concept of analogy has been applied by Iraqi judges, it means that judges can consider the act of the unlawful obtaining of another person's means of identification as theft by measuring it on the appropriation of electric power that is considered as a crime in existing theft offence laws. On the other hand, it may be subject to the law that governs the taking of another person's intellectual property because the conditions that the analogy requires are available in the obtaining of another person's means of identification.[88] The first condition, for instance, is the electric power, intellectual property, and a person's means of identification have similar elements. For example, they are intangible things, they can be taken by non-physical

---

[85] K S Gallant, supra, note 5, 26; *Morrissette v. United States*, 342 U.S. 246 (72 S. Ct. 240, 96 L. Ed. 288) (1952)

[86] K S Gallant, ibid 26

[87] Li Li, supra, note 8; C Elliott & F Quinn, supra, note 4, 23; *United States v. Devegter*, 198 F. 3d 1324, 1237-28 (11th Cir. 1999); *United States v. Woodard*, 459 F. 3d 1078, 1086 (11th Cir. 2006)

[88] *United States v. Lemire*, 720 F.2d 1327, 1336 (D.C Cir. 1983); *United States v. Bohonus*, 628 F.2d 1167, 1172 (9th Cir.) cert. denied, 447 U.S. 928, 1000 S. Ct. 3026, 65 L. Ed. 2d 1127 (1980); *United States v. Reece*, 614 F. 2d 1259, 1261 (10th Cir. 1980); *United States v. Bryza*, 522 F. 2d 414, 422 (7th Cir. 1975), Cert. denied, 426 U.S. 912, 96 S. Ct. 2237, 48 L. Ed. 2d 414, 422 (7th Cir. 1975); *H v CPS* [2010] EWHC 1374 (Admin) Division Court, in this case, the court extend the assault to encompass the assault that is committed against teachers in private schools; *Reginal v Unah* [2011] EWCA Crim 1837

means, and the taking of them does not deprive the owner of them.[89] The second condition is the taking of the electric power and intellectual property has been criminalised in the Iraqi statutes, while the obtaining of another person's means of identification is not.

It could be said that the use of the analogy as a means to criminalise the act of the unlawful obtaining of another person's means of identification is unacceptable to be adopted in Iraq because Iraqi judges are prohibited from creating a crime and setting out punishment for it by analogy. In *A v. K,* the Federal Court of Babylon confirmed that the analogy is prohibited in the Iraqi Penal Code 1969.[90] The creation of crimes and setting out punishments are considered violation of the principle of legality.[91] Hall[92] refuses to consider the analogy as a means to creating a crime. He pointed out that the use of the analogy to create a crime and set out a punishment is considered violation of the principle of legality. In addition, it has been claimed that the creation of crimes must be confined to the legislature. Consequently, judges should not create new crimes,[93] because granting the judges as a power to creating crime and its punishment may carry too a great risk of non-majoritarian crimes. Moreover, it may create a huge risk to people who may not know what behaviour is prohibited and what is not.[94]

It might also be said that prohibiting the Iraqi judge from creating crimes and set out punishments is not an uncanny principle. In UK, for instance, although there is no principle of legality as there is in Iraq as well as UK depends on the common law system, which empowers the judge a power to create law, the House of Lords, however,

---

[89] *United States v. Condolen*, 600 F. 2d 7, 8 (7th Cir. 1979); *United States v. Louderman*, 576 F. 2d 1383, 1387-88 (9th Cir.), Cert. denied, 439 U.S. 896 S. Ct. 257, 58 L. Ed. 2d 243 (1978)

[90] *A v. K*, Federal Court of Appeal of Babylon T/J/ 2012, 26/9/2012, 363 in this case the court has stated that the fine, which is stated in article 27(5) of the Guns Law and the section in decision No. 206 of 1994 is limited to possession of one type gun as opposed to every type, therefore, the analogy to creating a crime and setting out a punishment is prohibited.

[91] Interview with Dr. assistant Professor S Al Fatlawi, a lecturer and Deputy Head of School of Law, Baghdad University School of Law (Baghdad, 16 February 2013); interview with J K Maeen the Head of the first criminal group at Appeal Baghdad Federal Court, Appeal Baghdad Federal Court (Baghdad, 27 January 2013); interview with S AbdulHadi, a judge at Federal Court of Appeal of Diyala, Diyala Court, (Diyala, 25 January 2013); interview with B Obeidi, a prosecutor at Presidency of the Federal Court of Appeal of Diyala, Diyala Court (Diyala, 26 January 2013)

[92] J Hall, supra, note 27, 170

[93] C. Herman Pritchett, 'The Roosevelt Court: A Study in Judicial Politics and Values' 1937-1947, 240-63 (Macmillan 1948) cited in Li Li, supra, note 8

[94] William J. Stuntz, 'The Pathological Politics of Criminal Law' (2001) Vol. 100 Michigan Law Review 505- 576

in *R v Jones and Others* confirmed that the judge could not create a crime by using analogy.[95] The House of Lords stated that the main source of new criminal offences was the statute law created by Parliament. It added that the executive and judges had no right to create new offences in the ambit of criminal law. The House of Lords stated:

> ... (T)he court no longer had power to create new criminal offences; that as a matter of democratic principle it was for Parliament and not for the executive or judges to determine whether conduct not previously regarded as criminal should be treated as attracting criminal penalties, and, therefore, statute was the sole source of new offences.

In the same sense of the view of the House of Lords, it has been argued that judicial creation of the law is prohibited because the judge is not a legislator. The legislator is the only ones who has the right to create new offences in criminal law.[96] Moreover, the UK criminal judge prohibited from creating a crime by analogy because creating the crime by analogy is considered a breach of Article 7 of the European Convention on Human Rights.[97]

It might be said that if judges in UK, which espouses common law system, are prohibited from creation the crime and setting out a punishment for it, a fortiori, the Iraqi judge cannot use the analogy to criminalise an act that the legislature does not criminalise it.[98] Accordingly, the Iraqi criminal judge cannot use the analogy to extend existing theft offence laws (or to create a new one) to govern the act of the legal or illegal obtaining of another person's means of identification, and then using it to commit other crimes. He is prohibited from using the analogy to find a solution to fill in the gap not just in theft offence laws, but also in completely Iraqi criminal laws. This prohibition stems from the principle of legality, which is adopted by the Iraqi legislation. Using the analogy to criminalise identity theft as a specific crime is

[95] *Regina v Jones* and *Others* (2006) 2 WLR 772
[96] M Alraezki supra, note 16, 3
[97] M Jefferson, supra, note 46, 7
[98] *M v. K* [1970] Court of Cassation supra in this case the court of cassation stated that the café cannot be one of the places that were stated in article 263 of the Baghdadi Penal Code because there is no guard that lives in the café. In addition, the analogy is prohibited in criminal cases, so the café is subject to article 265 of Baghdadi Penal Code; *S V. H* [1971] Court of Cassation 1697, in this case the Court of Cassation has also stated that after the documents have been examined it was found that the garage is not one of the places that were stated in s5 of article 443 of the Iraqi Penal Code 1969. Due to the analogy is prohibited in penal cases the accused's behaviour is subject to s4 of article 443 rather than s5 of article 443 because there is a guard lives in it; *G v. D* [1970] Court of Cassation 286, in this case the court of cassation stated that criminal texts prohibit the expanding by analogy. Crimes that have been determined in the National Safety Law are stated as limited crimes, thus, a new crime cannot be added to them by using the analogy.

considered violation to the principle of legality.

It can be argued that it is unquestionable that the modern technology puts people's lives at risk; leaving their sensitive information more susceptible to being the target of crimes, such as theft and that needs to be countered by either the legislative or judicial solution. The current theft offence laws are inadequate to protect people's means of identification. In addition to this, it has been shown with the strong validity of the previous arguments that the judicial solution can be explored by interpreting the ambiguous legislation. Furthermore, this ambiguity may present an opportunity for the judges to extend such legislation, which is represented in this case by the current theft offence laws to govern identity theft.

However, it is difficult to confer upon the Iraqi criminal judges a power to extend existing theft offence laws (or create a new law) to govern identity theft because, Iraqi judges, contrary to the judges of the UK and US they have no experience in dealing with modern crimes, such as identity theft that are not covered by specific laws. The Iraqi judge should not be empowered with creation of new law principles irrespective of the principle of legality of which allows him to expand the scope of existing theft offence laws by interpreting them because Iraqi judges since a long time find a readymade solution for every crime. Identity theft is a new crime that they have encountered, thus, the creation of a new law to combat identity theft should be done within the scope of the legislature's function that is represented by Parliament. Therefore, the Iraqi legislature is requested to enact a new Act to deal with the act of the legal or illegal obtaining of another person's means of identification, and then using it to commit other crimes.

5.3 Conclusion

Due to Iraq having no specific law that governs identity theft the current theft offence laws have been analysed in the previous chapter. Having analysed theft offence laws it has appeared that they are inadequate and ineffective to govern identity theft. Therefore, this inadequacy needs to be solved by either judges or the legislature. In this chapter, the potential judicial solution to overcome the inadequacy that was determined in existing Iraqi theft offence laws has been discussed. Generally, it is showed that while

judges can plug gaps that may be found in their legislation their ability to create a new law is severely constrained.

Criminal law can sometimes seem ambiguous and unclear, thus, it needs interpretation. In different jurisdictions, most judges adopt some approaches to interpret the ambiguous statute. In Iraq, such other countries in civil law system criminal judges utilise several approaches: - literal, an extensive interpretation, and the approach of declaring the intention of the legislature.

To appreciate whether the Iraqi judge can interpret the current theft offence laws the study has attempted to examine the above approaches of the interpretation. The common rule in interpretation is that the statute should narrowly be interpreted. However, the narrow interpreting of the law may sometimes not achieve justice and enable the criminal to avoid being subject to criminal liability. After these three approaches have been examined, the study showed that the extensive interpretation might be the best means that can assist criminal judges to close the gaps in their legislation. However, in Iraq, using the interpretation of the statute by judges to overcome the legislative inadequacy that was determined in existing theft offence laws may be obstructed by the principle of legality.

The principle of legality consists of two parts: *nullum crimen* and *nulla poena sine lege.* These two parts of the principle of legality are considered more important in the scope of criminal law. Two results may be achieved by setting forth the principle of legality in both constitution and legislation. The first result is the principle of legality does not allow the legislature to enact a new law to govern a crime that has been committed in the past if it was not governed by the current criminal statute. The second result is it prevents the judge from applying the law retroactivity to govern crimes, which took place in the past. These outcomes are called *ex post facto law* prohibited and non-retroactivity principles.

The above consequences should be regarded as logical consequences of the principle of legality. According to the principle of legality, any interpretation that leads to creating a crime, increasing, or decreasing a punishment is considered unconstitutional and courts should not apply it. As a result of these two consequences, it has been shown that the law should not be enacted to govern crimes that took place beforehand because the

principle of legality serves to protect individuals. In addition, laws should be enacted by the legislature or any another entity that has an authority to enact law.

To assess whether the Iraqi judge can interpret the current theft offence laws in a manner that leads to extend the scope of them (or to create a new one) to cover identity, the role of the judge in dealing with elements of theft has been examined. With respect to the analysing of the term 'appropriation', the study showed that the Iraqi legislature does not define and determine it. Therefore, the Iraqi judge can return to language dictionaries or the history of legislation to explore the meaning of the term appropriation.

By analysing the term appropriation and making comparison between the role of Iraqi judge with the role of both the UK and US judges to interpret their legislation, the study showed that the Iraqi judge could interpret the term appropriation to include the act of the lawful or unlawful obtaining of another person's means of identification with intent to commit other crimes. By doing so, the Iraqi criminal judge does not violate the principle of legality and other principles that derive therefrom because there is no clear indication in Iraqi legislation that may refer to the obtaining of another person's property should be committed by physical means only.

The study also examined the role of the Iraqi criminal judge in interpreting the element of *mens rea* that is stated in the current Iraqi theft offence laws. The study showed that this element is also not defined by the Iraqi legislature. Since a judicial interpretation of statute does not oblige judges in lower courts or judges of courts in the same level, the author believes that theoretically there is no obstacle to be encountered when the Iraqi judge interprets the element of *mens rea* of theft offence stated in existing theft offence laws to expand the scope of it to govern the *mens rea* of identity theft. However, it has been shown that Iraqi criminal judges are reluctant to extend the meaning of *mens rea* of the traditional theft offence to meet the *mens rea* of identity theft.

After analysing both the elements *actus reus* and *mens rea* of the traditional theft offence, the author has attempted to examine whether the Iraqi judiciary can interpret the term 'property' to expand the scope of its meaning to govern a person's means of identification. It was shown that the Iraqi legislature in theft offence laws stated that the property as a subject of theft should be 'movable tangible property.' According to this

definition, two conditions have been required in things to be subject to theft: movable and tangible. Therefore, everything is not movable or tangible cannot be subject to theft. The study showed that by setting forth conditions like these in theft offence laws makes the term 'property' unambiguous. Consequently, the Iraqi criminal judge cannot expansively interpret the term 'property' to cover a person's means of identification because the means of identification is intangible and it cannot be moved from one place to another.

With respect to that whether it is appropriate the Iraqi judges can depend on the UK and US judges' experience, the study showed that Iraqi criminal judges cannot use the UK and the US judges' experience to extend existing theft laws (or to create a new law) to govern identity theft. The reason behind this is even the judges in these countries are currently prohibited from extending their existing laws (i.e., from creating new laws to govern new illegal activities not governed by existing laws.

In this study, a suggestion was presented, in which it was proposed that Iraqi judges should be prohibited from both creating a crime, and, increasing, or decreasing a punishment. He should be prohibited from doing same, even if modern technology puts people's lives at risk on account of the fact that nowadays their sensitive information is more susceptible to crimes, such as theft, because creating the law is a function of the legislature only. In addition, they have no experience in dealing with modern crimes, such as identity theft. It is not impossible to say that the legislature should amend or re-examine the provisions of the statute to be more appropriate to prevent unlawful acts that may be committed by using the new technology, such as the Internet.

The analogy as a means to fill in gaps that may be found in legislation, has also been analysed in this chapter to examine whether the Iraqi criminal judge can use the analogy to close the gap in the current theft offence laws. Having analysed the analogy it has appeared that the Iraqi criminal judge cannot use it to fill in the gap in the current theft offence laws because the analogy leads to creating a crime and set out a punishment for it. However, creating a crime or determining a punishment for it by the judges is prohibited by the principle of legality. As a result, the Iraqi legislature is required to enact a new law that deals with identity theft.

The study showed that judges of the UK and US could not expansively interpret theft

offence laws to extend their meaning (or to create new laws) to govern identity theft because the judges in these countries are also prohibited from creating a crime and setting out its punishment. Consequently, the US legislature has enacted two laws called identity theft laws that deal with identity theft. Whereas the UK legislation still suffers from the legislative inadequacy. The UK legislature does not consider identity theft as a separate crime. Therefore, UK courts may use some scattered provisions that are found in many laws to deal with identity theft.

A question remains is can the Iraqi legislature benefit from either the UK laws that indirectly deal with identity theft or the US identity theft laws to enact a new law to combat identity theft and methods that are used to obtain another person's means of identification. This issue will be discussed in the next chapter.

Chapter Six:

Adopting or Borrowing Legislative Solutions from Either UK or US Legislation or from both

Introduction

The two previous chapters have shown that the current Iraqi theft offence laws are inadequate to combat the identity theft offence and the Iraqi criminal judges could not overcome this inadequacy in existing theft offence laws. On other hand, the Iraqi legislature has not enacted a new law to combat this kind of crime. The Iraqi Government recently has proposed a new project that is called the Information Crimes Project of 2011, but the Iraqi Parliament has rejected this project.[1] It was shown in chapter four that this project is also inadequate to deal with the theft of personal and financial information of people. As a result, in this chapter, the study attempts to propose a new law to combat identity theft in Iraq.

In order to prepare this proposal, the chapter will analyse the legislative solutions that were presented by (both the UK and the US legislation) that were chosen as a reference in this study. By this analysing, the study will examine whether the Iraqi legislature can borrow or adopt provisions from both or from one of the UK and US legislation to fill in the gap in Iraq's legislation. It is not useful for the Iraqi legislature to 'copy and paste' the UK or the US legislation because there are huge differences between Iraq and these two countries in terms of economic development, ideologies, and cultural background. However, there is no doubt that the Iraqi legislature may benefit from the US and UK experience in order to enact a comprehensive law to govern identity theft.

In fact, the UK does not consider identity theft as a specific crime or a separate crime, thus, it has not enacted a specific law to govern it. Therefore, courts in the UK continue

[1] The Iraqi Parliament has rejected the Information Crimes Project of 2011because this project contains many provisions against the freedom of people. It also contains strict penalties. It is stated that this project prevents people, particularly journalists from writing or criticising the Iraqi Government. T Al Zarqani,'The Iraqi Parliament Abolishes the Information Crimes Project Due to not need it and Iraqis have Rejected, Agad Neze Wekala for News, It' 5 February 2013 available at <http://www.akadnews.org/مجلس-النواب-يلغي-قانون-جرائم-المعلوم/> accessed on 12 January 2014; the Abolishing of the Information Crimes Project Constitutes a Victory for Freedom Speech and It is Recorded by Iraqi Civil Society and the Iraqi Parliament, Iraqi Civil Society News, 6 January 2013 available at <http://www.almubadarairaq.org/?p=349> accessed on 12 January 2014

to apply many laws, such as the Data Protection Act 1998[2], Theft Act 1968[3], Fraud Act 2006[4], and Computer Misuse Act 1990[5] to a person who unlawfully uses another person's identity to commit other crimes. They may rule against the accused on fraud grounds, or hold that the person committed some other crimes, rather than identity theft *per se*. While in US, identity theft has been considered a federal crime under the Identity Theft and Assumption Deterrence Act 1998, also referred to the Identity Theft Act.

It seems that it is impossible to analyse and examine both the UK and the US approach in the same section because they vary greatly (the former has no specific provisions that deal with identity theft, whereas the latter has specific provisions that deal with identity theft). Consequently, the author intends to analyse and examine below in separate sections these two approaches to scrutinise whether and to what extent the Iraqi legislature can borrow provisions from one or from both of them to enact a comprehensive Act that deals with identity theft in Iraq.

6.0 Merits and Demerits of the Legislative Solution That the Iraqi Legislature Is Required to Adopt or Borrow Provisions from It

In order to criminalise the theft of a person's means of identification, the Iraqi legislature should define this type of crime or at least determine its elements. As was shown in chapter three, identity theft consists of two main elements: *actus reus* and *mens rea*, and a third element, which is a means of identification or what is referred to as the subject matter of crime. Consequently, in compliance with the principle of legality the Iraqi legislature needs to determine these three elements precisely. By doing so, the Iraqi legislature may need to adopt or borrow provisions that determine and cover these elements from either the UK or the US legislation or from both of them. As a result, the merits and demerits of the UK and US legislation will be discussed below.

[2] Data Protection Act 1998 c. 29 (UK)
[3] Theft Act 1968 c. 60 (UK)
[4] Fraud Act 2006 c. 35 (UK)
[5] Computer Misuse Act 1990 c. 18 (UK)

6.1 Can the Iraqi Legislature Adopt or Borrow Provisions from UK Legislation to Combat Identity Theft?

As stated previously, in the UK, there is no specific law that directly deals with identity theft because the UK legislature does not consider it as a separate crime. As a result, courts have resorted to many laws (such as the Data Protection Act 1998, Theft Act 1968, Fraud Act 2006, and Computer Misuse Act 1990) to find provisions that deal with crimes of identity theft. To examine whether the Iraqi legislature can benefit from these laws to legislate a new comprehensive identity theft offence law the above laws will be analysed in detail below.

6.1.1 Data Protection Act of 1998

In this section, provisions of the Data Protection Act 1998 will be analysed to scrutinise whether the Iraqi legislator can adopt or borrow some of them to combat identity theft. In 1998, the UK legislature enacted the Data Protection Act to protect individuals' information and prevent the unlawful use of it. It contains eight provisions that can be used to protect a person's information.[6] It was enacted to protect living persons only by preventing the abuse of their personal information.[7] It does not protect the deceased's information, whereas identity theft can be committed against both living and dead persons' means of identification. It also regulates and protects individuals' information, which is gathered by data controllers only. It does not regulate individuals' information in general. In addition, it requires data controllers to take reasonable measures that

[6] S1 of the Data Protection Act 1998 (UK), in this Act, it is stated that: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—(a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 4. Personal data shall be accurate and, where necessary, kept up to date. 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. 6. Personal data shall be processed in accordance with the rights of data subjects under this Act. 7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data; M Conradi, 'Legal Development in IT Security' (2007) Vol. 23 (4) Computer Law & Security Report 365

[7] R Dunnill and Ch Barham, 'Confidentiality and Security of Information' (2007) Vol.8 (12) Anaesthesia and Intensive Care Medicine 509-512

should keep them abreast of technological development.[8] The Data Protection Act of 1998 also requires data controllers to ensure the reliability of employees because those employees have control access to this information.[9]

The main issue that concerns this study is the crime that is created by the Data Protection Act. The Data Protection Act 1998 makes it as a crime if a person contravenes one of the provisions that are stated in the Act. The *actus reus* of this crime takes place when a person obtains or discloses a person's means of identification without a data controllers' consent or knowledge.[10] In addition, it considers selling or offering for sale personal information to other persons to be a crime if this information was obtained in contravention of section (1) of the Data Protection Act 1998.[11] However, the disclosure of an individuals' information contrary to section (1) of the Data Protection Act may not be a crime and the person may not be guilty of disclosure of an individuals' information if the revealer aims through disclosure the information to detect and prevent another crime.[12]

The *mens rea* of the above crime occurs when the accused intentionally or recklessly discloses a person's information. The Data Protection Act 1998 puts rules in place to prosecute data controllers when they intentionally or recklessly disclose a person's information, but not if they disclose such information coincidentally or unintentionally.[13]

It could be argued that the Data Protection Act 1998 is a regulatory law rather than a criminal law. It provides civil and administrative protection for personal information rather than criminal protection. In other words, there are civil and administrative

[8] J Frankland, 'Numeric Data Integrity: Piercing the Corporate Veil' (2009) Vol. 2009 (8) Network Security 11-14; S Hinde, 'Knowledge Is Power: Protecting Privacy' (2005) Vol. 2005 (7) Computer Fraud and Security 16-17

[9] M Conradi, supra, note 6

[10] S 55 (1) of the Data Protect Act of 1998 UK, [A] person must not knowingly or recklessly, without the consent of the data controller: (a) obtain or disclose personal data or the information contained data, or (b) procure the disclosure to another person of the information contained in personal data.

[11] S 55 (4): A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).
S 55 (5): A person who offers to sell personal data is guilty of an offence if—
(a) he has obtained the data in contravention of subsection (1), or
(b) he subsequently obtains the data in contravention of that subsection.

[12] Section (2) Data Protection Act of 1998 UK

[13] A Charlesworth, 'The Future of UK Data Protection Regulation' (2006) Vol.11 (7) Information Security Technology Report 46-54

remedies against the act of the illegally obtaining of such information from data controllers. However, according to criminal law view, criminal sanctions should be imposed if this information has been unlawfully obtained from the agencies that are gathering information about people, or the information has been disclosed by an employee of the agencies to other persons.[14]

Therefore, for the aforementioned reasons, the Data Protection Act of 1998 is inadequate in terms of protecting personal information from identity theft because identity thieves obtain personal information through many methods not just from the agencies or so-called data controllers. Due to the Data Protection Act 1998 regulates and protects people's information that is held by data controllers only, thus it cannot protect people's identities, which is stolen by thieves from people themselves. Nor does 1998 Act protect against the theft of identities of deceased persons or companies. In addition, penalties that are found in this Act are civil and administrative penalties rather than criminal penalties. As a result, it is inappropriate for the Iraqi legislature to adopt or borrow provisions from this Act to enact a comprehensive law to protect against the unlawful obtaining of personal and financial information in Iraq. The question therefore arises can the Iraqi legislature adopt or borrow provisions from other UK laws, such as the Theft Act 1968 due to this Act being more flexible than the current Iraqi theft offence laws?

6.1.2 Theft Act 1968

As shown in chapter four, although the Theft Act 1968 was enacted to deal with the illegal activities that may be committed against tangible and some intangible property, UK courts, however, stated that the Theft Act 1968 is ineffective and inadequate to govern *identity theft*. It is ineffective and inadequate because it was mainly enacted to deal with physical or tangible property, as well as some non-physical or intangible property. It was shown through some examples given in the analysis completed in chapter four, that identity theft does not fall within the scope of traditional theft, the

[14] S 55 (3) of the Data Protection Act 1998 UK, this Act has been amended by section 161 of the Criminal Justice and Public Order Act 1994. The section made the procurement and sale of computer held personal information knowing that it has been disclosed in contravention of the Act, a criminal offence. This may include advertisements and social engineering acts as an offence; Attorney General's Reference (No. 140 of 2004) [2004] EWCA Crim 3525; T Mulhall, 'Where Have all the Hackers Gone? Part 4- Legislation' (1997) Vol. 16 (4) Computer Law & Security Report 298-303

matter, which that Act, was enacted to deal with.

In effect, the author has found many difficulties in terms of actual situations in the UK. There is no explicit scholastic or jurisprudential view that confirms that the Theft Act 1968 contains provisions to effectively combat identity theft. Consequently, the Iraqi legislature cannot benefit from Theft Act 1968 because it suffers from the same lacuna that existing Iraqi theft offence laws suffer from.

UK judges also do not attempt to construe its provisions to expand them to govern identity theft, although in the past and sometimes in present time, judges in British courts have empowered themselves to designate a crime and its punishment. Below some cases are concerted in which although a criminal was found to have used another person's means of identification, nevertheless but the UK courts did not describe the unlawful use as identity theft. Courts focus instead on the unlawful activities that are committed by using the stolen identity, thus, they described it in various ways:

In *Yam v R,*[15] the court dealt with identity theft as fraudulent misuse of a dead person's identity and not as identity theft. As stated precisely, British courts judge the accused on fraud grounds or another crime rather than identity theft. The following is a descripting of the judge's sentencing:

> The judge passed a concurrent sentence of four and a half years for the burglary. That fell to be assessed on the hypothetical basis that the defendant had been the "fraudsman" but not the killer. The theft was of mail, from the owner's home. It was done with a view to wholesale manipulation of the victim's identity and bank accounts, which was the carried out over a period of three weeks or so. There is nothing arguably wrong with four and a half years, after trial, for such a burglary.

[15] [2010] EWCA Crim 2072; *Darwin & Anor, R v R* [2009] EWCA Crim 860:- in *Darwin & Anor, R v R*, the accused and her husband were facing in financial difficulties and were under pressure to meet debts due to credit card companies and mortgage providers. In 2001, the accused was taken out on his life. To cope with this situation they decided to commit fraud to obtain money from the insurance company. On 21 March 2002, the accused staged his apparent drowning at sea in a canoeing accident. To disguise himself he used the identity of a person who died in childhood, and then lied his way into a new identity by obtaining a driving licence, passport and all the necessary documents required for modern living. In effect, he successfully managed to live with this false identity, undetected; *Sammon v R* [2011] EWCA Crim 1199:- according to the facts in this case the accused was suspected of fraud and had been arrested by police. He posted bail and was waiting for trial. "He breached his bail and ever since had remained at large," thereafter he was absently convicted by the court. During his absence, he used his deceased friend's identity to disguise himself. When he was arrested by police, he was convicted by the court on other offences rather than identity theft.

In *Sofroniou v R*,[16] although the accused had used another person's identity to defraud or attempt to defraud banks and credit cards companies to provide him bank services or other services the court did not judged the accused on identity theft. It just pointed out that the crime against the accused had been labelled by the prosecution as identity theft. As will be shown in the next section, under US laws, the accused may be guilty of both identity theft and obtaining property by deception. It could be said it would be considered more important if the UK courts clearly held that the use of another person's means of identification is a means to commit crime because they hesitate to consider it as a crime.

Gobbons and others v R[17] is another case that related to identity theft. In this case, the accused used dead persons' identities and names of innocent members of the public and redirected their mails to receive information about them to defraud banks and credit card companies to obtain cash, property, and services. According to current definition of identity theft, the illegal activities that are committed by the accused constitute identity theft, but the court did not prosecute the accused on identity theft grounds. However, the court instead convicted him of conspiracy with others to obtain property by deception according to section 15 of the Theft Act 1968.[18]

In *Sward v R*,[19] the judge in his discussion referred to identity theft, but it is noted there

[16] [2003] EWCA Crim 3681 in this case, the accused was charged with obtaining services by deception contrary to section 1(1) of the Theft Act 1978. The accused falsely pretended to be Andrew Cole, John Groves, or Andrew Narramore to deceive or attempt to deceive banks into providing him with banking services, credit card companies into providing him with credit cards, and retailers into providing him with goods.

[17] [2002] EWCA Crim 3161 [2003] 2 Cr App Rep (S) 34 [2003] Crim LR 419 [2003] 2 Cr App R (S) 34

[18] "……(W)ere convicted of conspiring together with others unknown to defraud banks and credit card companies by dishonestly obtaining the redirection of mail, applying for credit account facilities by giving false details about themselves by telephone and in writing and using the fraudulently obtained credit cards to acquire goods, services and cash, contrary to common-law".

[19] [2005] EWCA Crim 1941. In this case, the accused or someone with whom he was acting in concert made or caused to be made a phone call Barclays Bank call centre in March 2004 pretending to be Mr James Turner, who had an account bank with Barclays Bank, asking them to send a premier account card to a branch in Leeds. The card was sent by the bank. In addition, the accused supported his request to get this card by a false driver's license in Mr James Turner's name. The card was delivered to the accused by an employee of the bank. The accused signed the card with the same signature found on the false license. At or about this time, Mr James Turner transferred the sum of £20,000 to the account, from which funds were to be drawn by a premier card. There is no indication that the accused and his associate knew of the transfer of money. After this, the accused withdrew £4,500 from Mr James Turner's account from a Barclay's branch in Wakefield. Then he went to Mansfield and obtained £5,500 from another branch of Barclays. In another attempt, he went to Nottingham and tried to withdraw £5,000, but he discovered when the alert cashier observed that the paper of the false licence was of poor quality and subsequently dubious appearance and arrested.

was no clear sentence for this crime. His sentence was as follows:

> ….. [A]nd for four charges of using a false instrument he was sentenced on each to two-and-a-half years' imprisonment. All those sentences were ordered to run concurrently. In granting leave the single judge observed that there was a paucity of authorities for this kind of offence. The kind of offence the learned single judge was referring to was identity theft, of which this is a typical example.

Although the case of *Olden, R. v R*[20] falls, according to the current concept of identity theft, within the scope of identity theft, the court ruled against the accused on a crime of obtained properties by deception grounds. In the court's decision, there was no indication of the ways in which the accused obtained these names, and then used them to gain property. If the act of the unlawful obtaining of a person's means of identification is a crime according to the Theft Act of 1968, then a court can prosecute the accused on both identity theft and the obtaining of property by deception grounds. However, it seems that the unlawful obtaining or using another person's identity is not branded as identity theft in the Theft Act 1968.

In *R. v Ayodele Odewale and Others,*[21] there also was no any indication of the elements

[20] [2007] EWCA Crim 726:- in this case, the accused used other persons' names, such as Trevor Paul Ellis and Martin Dubrey to obtain two passports. In addition, he used Terence Leslie Batters' identity to obtain a driver's license. Moreover, he set up bank and building society accounts and applications for mortgages and unsecured and secured loans using those names.

[21] [2004] EWCA Crim 145; the *R v Williams* case deals with a different issue: - The main offences in this case were acquiring, using or having criminal property contrary to section 329 of the Proceeds of Crime Act 2002 and two counts of concealing, disguising, controverting or transferring criminal property contrary to section 329 of the Proceeds of Crime Act 2002. However, the court pointed out that... The method that have used had involved obtaining and using the identification details of that customer and this appellant had allowed himself to be used by assisting in opening a fraudulent account and then withdrawing £10,000 and attempting to withdraw another £5,000….the fact in this case is in August 2008 the accused fraudulently assisted another person who falsely hold himself out to be the customer "Neil Carson" and they transferred approximately £20.000 of his account. The judge stated that certain crimes were becoming increasingly common and struck at the heart of the banking system and caused great distress to victims. The identity of innocent people was stolen and substantial sums were taken from their accounts. [2009] EWCA Crim 2194; although *Pigott v R,* does not relate to identity theft, the author discussed it here to prove that neither the UK legislature nor the UK courts consider the obtaining of a person means of identification as a separate crime. The main point in this case, was the sentence of confiscation against to accused. The Crown Court when intended to impose the confiscation stated many facts. In its verdict, the court stated that the accused used a false identity to gain benefit. In effect, the accused did not use a false identity. He used a real identity that belonged to a dead person called Chapman. He obtained Chapman's identity from a gravestone near his place of birth. In addition, he had an offshore Jersey account with Lloyds TSB in the name of Chapman. He also used that name to open bank accounts in Hong Kong. He used the name TJ Power to open an account with HSBC Bank. He had a driving licence, birth certificate, and medical card in that name. It was alleged that he also used the identity of Daniel Anthony Clifford in connection with 'Qualinorld' (a company used in the fraud). He also used companies' identities some of these companies are false whereas the others are true. It can

of identity theft; methods that were used to obtain occupants' means of identification, the court held that the criminals were guilty of conspiracy to defraud financial institutions by means of identity theft. The court stated only that:

> [T]he identity of the former occupants would be established and false documents such as driving licences or utility bills were obtained. These were used to open accounts with a bank or building society, and loan facilities including credit and debit cards were obtained. Arrangements were made to divert mail and telephone calls to the addresses and mobile phones associated with the conspirators.

In the above case, the Court of Appeal stated that: '[o]n 24th of March 2003 these appellants were convicted of conspiracy to defraud financial institutions by means of identity theft'. If identity theft as a means to commit other crimes this means that identity theft is not a crime in the UK. It appears from the decision of the Crown Court that neither the UK legislature nor UK courts consider the use of another person's means of identification as a punished crime. If the illegal use of another person's means of identification is a crime according to the UK legislation, the UK courts cannot violate or ignore the application of the law on this point. In this circumstance, the Iraqi legislature cannot benefit from the legislation does not consider the act of the illegal obtaining of a person's means of identification as a crime.

6.1.2.1 Usefulness of the 1968 Act for the Iraqi Situation

The Theft Act 1968 has been analysed as a reference in chapter four related to the scrutiny of the issue whether the current theft offence laws in Iraq are adequate to

---

be argued that all the aforementioned facts related to identity theft according to the current definition of identity theft, but the Crown Court did not take them into account when it branded the unlawful activities committed by the accused as a crime. At the court, the appellant pleaded guilty to one count of cheating the public revenue and one count of assisting another to retain the benefit of criminal conduct. He was sentenced to nine years imprisonment (later reduced on appeal to eight years), disqualified from directing a company for 15 years, and a confiscation order was made for £1,498,887.60, with 10 years' imprisonment in default. The appellant had been involved in a missing trader intra-community carousel fraud, involving a loss to the Revenue in excess of £40 million. The Crown Court did not charge accused on fraud. It reasoned its decision that the accused was not a main beneficiary of the fraud. It stated that the accused and his co-accused were a team operating in the execution of the fraud. [2009] EWCA Crim 2292 [2010] 2 Cr App Rep R (S) 16 [2010] 2 Cr App R (S) 16 [2010] Crim LR 153 [2010] LIoyd's Rep FC 97. According the legislation of some states, such as Canada, and Australia that criminalise the act of the unlawful obtaining of people's identities and scholars' literature, the identity of a person whether he is alive or dead is considered a real identity, and the use of it with the intent to commit other crimes is branded as identity theft.

govern identity theft. However, it is examined in this chapter in order to scrutinise all UK laws and examine whether the Iraqi legislature can borrow provisions from them to enact a comprehensive law to combat identity theft. Although in the Theft Act of 1968, the legislature has expanded the term 'property' as a subject of theft to encompass some intangible things, the aforementioned examples showed that the Theft Act 1968 suffers the lacuna and it is inadequate to deal with identity theft. Consequently, this Act, like the current Iraqi theft offence laws, is inadequate to govern identity theft.

It might be said that the Theft Act 1968 may also be inadequate and ineffective to assist the Iraqi legislature in combating of identity theft because it suffers the same lacuna that the current Iraqi theft offence laws suffer from. Therefore, the Iraqi legislature cannot adopt or borrow provisions from it to enact a new law to protect the personal and financial information of people from the illegal obtaining and then using to commit other crimes. The study will now attempt to analyse another law that may be used by British courts to fight identity theft. This law is the Fraud Act 2006.

6.1.3 Fraud Act 2006

In this section, the provisions of the Fraud Act of 2006 will be analysed to scrutinise whether the Iraqi legislature can borrow or adopt some of them to combat identity theft. The Fraud Act 2006 came into force on 15 January 2007. It aims to deal with all fraudulent activities, whether on or offline. Therefore, it defines a general fraud offence in section 1.[22] The Fraud Act contains three categories of offences: fraud by false representation (section 2), fraud by failing to disclose information (section 3) and fraud by abuse of position (section 4).[23] Some scholars and professionals stated that the analysis of the provisions of the Fraud Act 2006 shows that this Act deals with the wrongful conduct, rather than the result of a crime.[24] To appreciate whether the above

[22] The UK legislature in s1 of the Fraud Act 2006 stated that (a) person is guilty of fraud if he is in breach of any sections listed in subsection (2) (which provide for different ways of committing the offence).
(2) The sections are— (a) section 2 (fraud by false representation); (b) section 3 (fraud by failing to disclose information), and; (c) section 4 (fraud by abuse of position).

[23] Ss (2, 3, 4) Fraud Act 2006 (UK)

[24] M Johnson and K M Rogers, 'The Fraud Act 2006: The E-Crime Prosecutor's Champion or the Creator of a New Inchoate Offence?' 2007, 1-9 available at <http://www.bileta.ac.uk/content/files/conference%20papers/2007/The%20Fraud%20Act%202006%20-%20The%20E-Crime%20Prosecutor%27s%20Champion%20or%20the%20creator%20of%20a%20new%20inchoate%20offence.pdf> accessed on 29 May 2012; A Savirimuthu and J Savirimuthu, 'Identity Theft and System

sections can properly cover identity theft and whether they are adequate to be borrowed, or adopted by the Iraqi legislature, these sections will be analysed.

Section 3 of the Fraud Act 2006 deals with a crime consists of three elements: the accused should be under a legal duty[25], failing to disclose information to another person, and dishonestly that person fails to disclose this information to another person. If a person is under a legal duty holds information of another person and he is requested to disclose the information that he holds to a third party, such as a government, a company or the police, but he dishonestly fails to disclose this information to benefit himself or another or expose that person to risk, he may be guilty of fraud.[26] The question that may arise here is do the elements of the above crime meet the elements of identity theft.

As was shown in chapter three, a person is guilty of identity theft if he obtains, sells, uses, or transfers another person's means of identification without the rightful person's consent, with the intent to commit other crimes.[27] The accused under section 3 of the Fraud Act 2006 legally obtains the information. He already held this information. He does not transfer, sell, or use this information without the person's consent. He also has no an intent to transfer or to use it to commit other crimes. However, he fails to disclose the information that he holds to another person. The failing to disclose the held information is not an element of identity theft. Therefore, this section cannot be applied to identity theft because the elements of the crime that is under it do not meet the elements of identity theft. The Iraqi legislature cannot borrow or adopt this section if it intends to enact a new law to govern identity theft. The author now intends to analyse another section of the Fraud Act 2006 to find provisions in it that may assist the Iraqi

---

Theory: The Fraud Act 2006 in Perspective' (2007) Vol. 4 (4) Scripted 440 available at <http://www.law.ed.ac.uk/ahrc/script-ed/vol4-4/savirimuthu.pdf> accessed on 15 July 2012; M Jefferson, *Criminal Law*, (10th edn, Pearson Education Limited 2011) 629

[25] Persons may be under a legal duty, such as officials in banks, universities, or government institutions. Those persons may hold people's information. The legislature sometimes obliges them to disclose this information to the police or any other persons. If those persons are requested to disclose this information, but they refuse to disclose it to make a gain for themselves or for another, or to cause loss to another or to expose another to a risk of loss, they may guilty of fraud offence.

[26] A person is in breach of this section if he— (a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and (b) intends, by failing to disclose the information— (i) to make a gain for himself or another, or (ii) to cause loss to another or to expose another to a risk of loss.

[27] Identity theft consists of three elements: *actus reus*, which consists of the act of the illegal obtaining of a person's means of identification, the use of, or transfers of this information, the *mens rea* of identity theft and a person's means of identification.

legislature to enact the new law of identity theft.

The fraud offence under section 4 deals with the abuse of position to obtain gain or cause loss to another person.[28] Under section 4, a person may be guilty of fraud offence if he occupies a position, and then dishonestly abuses this position. Two elements should be available to accuse a person who abuses his position: (1) occupying a position and (2) dishonesty he abuses it to gain for himself or for another. The person should occupy a position in which he is expected to safeguard, or not the financial interests of another person, such as a government, bank, or a company. Then he dishonestly abuses this position to gain for himself or for another, to cause loss for another, or to expose another to risk or loss. The same question that has risen with respect to section 3 may arise here can section 4 of the Frau Act 2006 govern identity theft.

As stated in chapter three, criminals can obtain people's identities through various methods whether tradition or non-traditional, and then use them to commit other crimes. Abusing the position and misusing the information that is entrusted to a person is one of many traditional methods that are used to commit identity theft.[29] For example, a person who occupies a position in an institution, such as a bank, company or a government institution may be guilty of identity theft, if he abuses his position and obtains, sells, or uses personal information that is held by the institution to obtain a gain for himself or for another person. If the previous elements of the crime that created by section 4 have been compared to the above elements of identity theft, it appears that section 4 of the Fraud Act may govern only the act of the unlawful obtaining of personal information

[28] Section 4 of the Fraud Act 2006: Fraud by abuse of position(1)A person is in breach of this section if he—
(a)occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,
(b)dishonestly abuses that position, and
(c)intends, by means of the abuse of that position—
(i)to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.
(2)A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.

[29] As was shown in chapter three of this thesis, identity theft consists of two main elements: *actus reus*, which consists of the act of the illegal obtaining of a person's means of identification, the use of, or transfers of this information, the *mens rea* of identity theft and a person's means of identification, which may be a subject of theft. A person's means of identification can be illegally obtained by two ways: traditional and none traditional methods. One of these traditional methods is theft inside the work. A person is guilty of identity theft if he obtains or transfers, sells, or uses, another person's means of identification that he holds.

that is committed by the person who has been entrusted to hold this information.

It might be said that section 4 of the Fraud Act 2006 cannot assist the Iraqi legislature to create provisions to combat identity theft because the misuse of the position to commit identity theft is one of many methods that can be used to commit identity theft. In addition, in Iraqi legislation, the violation of the trust is considered a crime of betrayal trust and not theft. A betrayal of trust crime takes place when the information is submitted to the person according to his position, and then he misuses it to obtain illegal benefits for himself or for another.[30] The legal text to be appropriate (and then it could be suitable for adoption by the Iraqi legislature) should determine the distinctive features of the elements of identity theft. However, section 4 has not determined the elements of identity theft. It seems that the main section in the Fraud Act 2006 is section 2. A question may be risen here is section 2 of the Fraud Act 2006 providing adequate guidance for the Iraqi legislature to combat identity theft or it is unsuitable like both sections 3 and 4 of this Act.

Section 2 of the 2006 Act mentions certain elements of a fraud offence, such as a false representation and the state of mind of perpetrator. A person, to be guilty, must make a false representation with an intention to create a gain for himself or for another person, to cause loss to another person or to expose that person to a risk of loss.[31]

According to the circumstances stated above, the offence of fraud by a false representation consists of two components: *actus reus* and *mens rea*. The false representation represents the *actus reus* of the fraud offence. The UK legislature in section 2 of the Fraud Act 2006 defines the term false representation as any representation whether relating to fact or law, including a representation as to the state of mind of the perpetrator or that of another person.[32] The false representation may be untrue or misleading.[33] It does not matter how the false representation was conducted.[34] It may be silent or spoken, written or made by conduct. It may be explicit or implied.[35]

---

[30] Section 453 of the Iraqi Penal Code 1969
[31] S2 (1(a, b)) Ss (2, 3, 4) Fraud Act 2006
[32] S 2 (3 a, b) ibid; *King v DPP* [2008] EWHC 447 (Admin)
[33] S 2 (2 (a)) ibid
[34] S2 (4)Fraud Act 2006
[35] J Herring, *Criminal Law* (7th edn, Palgrave Mcmillan Law Masters UK 2011) 224; *R v. William* [1980] Crim LR 589; *R v Lambie* [1982] AC 449

It may be sent by post or an email.[36] The false representation is the main element in the offence of fraud that is stated in section 2 of the Fraud Act 2006. Therefore, there is no fraud if there is no false representation. In this case, the accused may be guilty of attempted fraud or another crime, but not fraud.[37]

The gain and loss constitute aims of the false representation. The gain occurs when the criminal obtains benefit for himself or for another person, whereas the loss occurs if the criminal causes loss to another person or expose that person to a risk of loss.[38] *Gain* is defined as keeping what one has, or getting what one does not have. When the criminal makes a false representation, he should obtain money or property. *Loss* means loss by not getting what one might get or parting with what one has.[39] The above elements are the main elements of the *actus reus* of the false representation offence that is stated in section 2 of the Fraud Act 2006.

On this point, section 2 of the Fraud Act 2006 has been criticised by some scholars[40] because it does not define the terms, *fraud* or *false*.[41] This section also has criticised because the fraud or false representation that constitutes the *actus reus* of the general fraud offence is considered too broad. Consequently, a person may commit the *actus reus* of the offence of fraud, even if he does not send the false representation via email to the victim, if he makes a false representation and knows that it is or may be untrue or misleading.[42] The question remains is, do these elements satisfy the elements of the *actus reus* of identity theft, and therefore can it be borrowed or adopted by the Iraqi legislature.

In fact, the elements of identity theft are ambiguous. Most legislation around the world does not state the methods that may be used to obtain a person's means of identification as elements of identity theft offences. Most legislation criminalises the stage after the commission of identity theft, such as the transferring of, or the use of, a person's means of identification only. However, as shown in chapter three of this thesis, scholars and

[36] S 2(5) Fraud Act 2006
[37] C Withey, 'Comment: The Fraud Act 2006- Some Early Observation and Comparison with Former Law' (2007) Vol. 71 Journal of Criminal Law 220-237
[38] S 5 Fraud Act 2006 UK
[39] S 5 (3, 4) ibid
[40] M Johnson and K M Rogers, supra, note 24, 1
[41] ibid 1
[42] M Johnson and K Rogers, supra, note 24, 4

professionals stated that identity theft could be committed by using two types of methods: the traditional or simple, and the non-traditional or sophisticated methods. Some sophisticated methods, such as phishing, or spam, may be caught within the false representation that is a requirement under section 2 of the Fraud Act 2006.

6.1.3.1 Some Identity Theft Acts That Could Be Covered by the 2006 Act

The criminal sometimes, for instance, uses phishing to trick people into revealing their means of identification, and then uses it to commit other crimes subsequently. The false representation in phishing occurs when a phisher sends bogus emails to unsuspecting victims, which resemble emails that are sometimes sent by trusted institutions, such as banks or companies. After receiving these emails, victims may reveal their sensitive information, such as credit card details or passwords. In this case, the *actus reus* of the offence of fraud is fulfilled if the bogus emails access the given website and have been received and read by the victims.[43] Therefore, it can be argued that the above provisions of section 2 of the Fraud Act may cover the act of phishing.[44]

Some scholars[45] stated that provisions of section 2 of the Fraud Act 2006 might also cover pharming. Pharming refers to transferring genuine emails that are sent to a genuine website to a bogus one [46] in order to change their contents, and then resend them to the users to dupe them into revealing their means of identification. On the other hand, it has been said that section 2 of the Fraud Act 2006 is not being applied to instances where a person surreptitiously installs spyware on a user's computer without his consent, because there is no false representation made that can be used to defraud the user legally. Bainbridge[47] stated that

> Section 2 does not appear to apply to spyware (software surreptitiously installed on a computer used to gather information without the user's knowledge).

[43] A Savirimuthu and J Savirimuthu supra, note 24, 440
[44] M Johnson and K Rogers, supra, note 24, 1
[45] M Johnson and K M Rogers, 'The Fraud Act 2006: The E-Crime Prosecutor's Champion or the Creator of a New Inchoate Offence?' 2007 available at <http://www.bileta.ac.uk/content/files/conference%20papers/2007/The%20Fraud%20Act%202006%20-%20The%20E-Crime%20Prosecutor%27s%20Champion%20or%20the%20creator%20of%20a%20new%20inchoate%20offence.pdf> accessed on 12 January 2014; D Bainbridge, 'Criminal Law Tackles Computer Fraud and Misuse' (2007) Vol. 23 (3) Computer Law & Security Report 276-281; A Savirimuthu and J Savirimuthu, supra, note 24
[46] D Bainbridge, ibid
[47] D Bainbridge, ibid, 277

> Spyware is installed on a computer's hard disk without the owner or user's knowledge. Therefore, no representation is made unless. It could be argued that there is an implied representation that the site from which it was 'sent' would not install spyware or other malicious software. This seems to be stretching the language of section 2 too far. However, it may be said that there is implied representation if the website that is used to send spyware does not install spyware or uses other malicious spyware.

It could be said that section 2 of the Fraud Act in this case is applied to methods that are used to commit identity theft and not identity theft itself. It cannot prevent or combat identity theft because there is difference between identity theft as a crime, and methods that are used to commit it. In addition, identity theft is not committed by using sophisticated methods only. It may be committed by either traditional or non-traditional methods. In most traditional methods that are used to commit identity theft, there is no false representation, which is the core ingredient of fraud offences under section 2 of the 2006 Act.

6.1.3.2 The Subject Matter of (False Representation) Under the Act 2006

The UK legislature in section 2 of the Fraud Act 2006 states that a person is guilty of a false representation if he intends by the false representation to obtain money or property. This issue may cause a problem when the *actus reus* of false representation is applied to identity theft because there is no agreement among scholars or judges whether a person's means of identification is considered to be property. Therefore, this section cannot be applied to the person who sends a bogus email to users in order to swindle them into divulging their personal information.

However, when the fraudster sends a bogus email in order to commit the identity theft offence, he has two intentions: - a direct intention and an ulterior intention. The direct intention is to obtain details about a person, such as his name, address, or his credit card information, while the ulterior intention is to use this information to commit other crimes, such as fraud or avoiding arrest by the police.[48] According to the literary meaning of section 2, the direct intention (to send the bogus email) may not be satisfied

[48] A. Steel, 'the True Identity of Australia Identity Theft Offences: A Measured Response or Unjustified Status Offences?' (2010) Vol. 33 (2) UNSW Law Journal 503-531

because personal information is not property. Consequently, the *actus reus* of the fraud offence (that is stated in section 2) is not satisfied.

Nevertheless, there is one circumstance in which the *actus reus* of the fraud offence may be satisfied, if the second part of the *mens rea* 'to expose another person to risk or loss' has been taken into account. The person may be exposed to risk or to loss if the criminal obtains their means of identification, and then uses that to commit other crimes, such as avoid arrest by the police or to commit fraud. In addition, it is stated that to apply this section there is no need to prove that the accused in effect gained, or caused, a loss.[49] For instance, if the accused sent a phishing email to unsuspecting victims asking them to send money to an account, it could amount to fraud (even if the victims who received the email deleted it. Moreover, as stated, the Fraud Act 2006 criminalises the conduct rather than the result. As a result, the accused commits an offence of identity theft even if the means of identification is not property.

It might be said that provisions of section 2 of the Fraud Act 2006 are inadequate to cover all methods that are used to commit identity theft, thus it cannot be used to effectively combat and prevent identity theft. However, there is one way in which the provisions of section 2 of the Fraud Act can cover identity theft (even if it does not cover all the methods that are used to commit it), if identity theft has been considered as a means to commit other crimes, such as fraud or obtaining property by deception. In this case, the criminal makes a false representation when he uses another person's means of identification to obtain property or money belongs to other persons.

It could be said that although section 2 has flaws, it may be workable for the Iraqi legislature because it has certain advantages, which may inspire the Iraqi legislature when it intends to enact a new identity theft Act or a Computer Misuse Act. The UK legislature in this section criminalised the conduct rather than the result. By criminalising the conduct, the provisions of this section could contain sophisticated methods, such as phishing, spam, or pharm. As was shown in chapter three most these methods are committed by a false representation.[50] Section 2 of the Fraud Act in this

[49] J Herring, *Criminal Law: Text, Cases and Materials* (4th edn, Oxford University Press 2010) 225

[50] For example, if the criminal uses phishing as a means to obtain a person's identify he may pretend as a legitimate entity, such as the person's bank. in this case, the can may be a subject to section 2 of the Fraud Act 2006

case may also cover some traditional methods that are used to commit identity theft, such as social engineering[51]; as a result, the Iraqi legislature can borrow or adopt section 2 when enacting a new law to combat identity theft. However, it should avoid the shortcomings that were determined previously in this section.

6.1.3.3 *Mens Rea* under 2006 Act

The *mens rea* of the fraud offence by a false representation takes place when the accused dishonestly makes a false representation with the intent to make a gain for himself or for another, or to cause loss to another person or to expose that person to risk.[52] The 2006 Act does not define the term 'dishonesty' because the legislature may intend to adopt the definition that is stated in the Theft Act 1968.[53] However, the definition of the term 'dishonesty' that is set out in the Theft Act 1968 is considered unsuitable to apply to the term 'dishonesty' that is stated in this section.[54]

Mens rea of the fraud offence by a false representation also occurs if the accused knows that the representation is or may be untrue or misleading.[55] However, the accused may not be guilty of the fraud offence by a false representation, even if he knows that the representation is untrue or misleading if the representation has innocently been conducted. The same question that has arisen with respect to the *actus reus* may be raised regarding the *mens rea* of identity theft: does the *mens rea* of the fraud of the false representation satisfy the *mens rea* of identity theft?

There is no dispute that the criminal, when he uses some methods, such as phishing, spam, or social engineering to obtain a person's means of identification, he makes a false representation. He knows that this representation is untrue or may be misleading. He also has an intention, when he makes the false representation, to benefit himself, or another person, or to expose that person to risk or to loss. As a result, the *mens rea* of the false representation offence meets the *mens rea* of some methods, such as phishing,

[51] Social engineering is a mean to persuade and convince individuals to disclose their personal information to the criminal. In this way, the criminal may pretend as a clerk in a bank or a company and then ask people about their information. It may be used on or offline by the criminal to obtain people's information.
[52] S 2(1(a, b))Fraud Act 2006 S 2(1(a, b))
[53] M Jefferson, supra, note 24, 629; J Herring, *Criminal Law: Text, Cases and Materials* supra, note 49 573
[54] M Johnson and K M Rogers, supra, note 24, 1
[55] S 2 (2 (a, b)) Fraud Act 2006

pharming, spam, and spoofing, but it does not meet the *mens rea* of other methods that are used to obtain a person's means of identification. The *mens rea* of the false representation could meet the further *mens rea* of identity theft, which is represented by an intention to use another person's means of identification to commit other crimes. According to the above analysis, the UK legislature does not offer comprehensive solutions to identity theft challenges that may face courts when they apply fraud offence laws to identity theft.

6.1.3.4 Overall Relevance of the 2006 Act to Help the Iraqi Situation

To sum up the previous analysis of the provisions of the Fraud Act 2006, it could be said that these provisions are useful although they do not provide *comprehensive guidance* for the Iraqi legislature to amend the Iraqi Fraud Act. Most Iraqi legislation was enacted since 1969. Few amendments were made to this legislation during the Saddam regime because there was no technology could be used in Iraq at that time that could give rise to identity theft offence. Now Iraq does not need an Act to govern only identity theft. It needs some laws to deal with the new crimes that have emerged from the new technology, such as online gambling, identity fraud and the computer misuse. Therefore, the provisions of the Fraud Act provide some provisions to combat sophisticated methods that are used to obtain individuals' information and online fraud.

The author realises that there is no Act in the world that can be enacted without some drawbacks. Consequently, the author observes that the determination of the drawbacks of the provisions of the 2006 Act will encourage the Iraqi legislature to avoid them when it intends to enact a new Act whether to combat identity theft or fraud in general. On the other hand, the author in his analysis of the provisions of the Fraud Act has found in each section some advantages, which may not be found in the US identity theft laws as will be seen in the next section. These advantages can be used to combat not all methods that are used to commit identity theft, but some of them. As was shown in chapter three the information of individuals can be obtained by two ways: sophisticated and non-sophisticated methods.

The main result achieved by the UK legislature in the 2006 Act was it has created in

section 1 a general rule of fraud.[56] This rule cannot be found in Iraqi fraud laws. It takes into account the accused's conduct rather than the result of that conduct. This will assist the Iraqi legislature to set out this rule if it intends to amend the current Fraud Act 1969. It might be said that section 2 of the Fraud Act 2006 UK has huge advantages that the Iraqi legislature can benefit from them,[57] but it is inadequate to provide a comprehensive solution that can be used to combat identity theft. However, even if the provisions that are stated in section 2 of the Fraud Act 2006 do not present *a comprehensive solution* to combat identity theft, they may provide some insight to the Iraqi legislature on how to amend its legislation, particularly fraud laws and theft offence laws.

Section 2 provides guidance for the Iraqi legislature to criminalise some sophisticated methods, such as phishing, spam, and pharming. Accordingly, it is proposed by the author that the Iraqi legislature can adopt or borrow these provisions after it avoids the shortcomings that appeared in them. As it was previously mentioned in this section the UK courts can also use section 4 to charge criminals of identity theft who hold people's means of identification, and then misuse them to gain for themselves or for another or expose those people to risk. This is one way of many that can be used by identity thieves to obtain people's means of identification, and then use them it to commit other crimes. Although this section covers one way of traditional ways, it inspires the Iraqi legislature that some traditional ways should be criminalised.

However, even with the above solution, the Iraqi legislature still need more precise provisions that can be used to combat identity theft because this solution is inadequate to cover some other methods, such as hacking, viruses and traditional methods that are used to commit identity theft and contain no false representation.

As it has been shown previously, in the UK, there is no specific law to govern identity

[56] the UK legislature in section (1) of the Fraud Act 2006 states that (a) person is guilty of fraud if he is in breach of any of the sections listed in subsection (2) (which provide for different ways of committing the offence).

[57] the UK legislature in section 2 of the Fraud Act 2006 states that (f)raud by false representation (1) A person is in breach of this section if he—
(a)dishonestly makes a false representation, and (b)intends, by making the representation— (i)to make a gain for himself or another, or (ii)to cause loss to another or to expose another to a risk of loss.

theft because it is not a separate crime under UK criminal law.[58] Consequently, if the courts do not find in previous laws, rules to govern the theft of a person's means of identification, they may resort to other acts, such as the Computer Misuse Act 1990 to find provisions to cover other aspects of this crime. This Act relates to computer misuse, thus, it may cover some methods, such as phishing, and pharming that were covered by the Fraud Act 2006. A question may be triggered here is can the Iraqi legislature adopt or borrow provisions from the Computer Misuse Act 1990.

6.1.4 Computer Misuse Act 1990

The Computer Misuse Act 1990 came into force on 29 August 1990. It deals with three categories of offences. At first glance, these categories overlap with one another. These categories are found in sections 1, 2, and 3 of this Act.

6.1.4.1 Could Section 1 of the Computer Misuse Act 1990 Adequate to Be Borrowed by the Iraqi Legislature

Section 1 of Computer Misuse Act defines a basic 'hacking' offence. It considers unauthorised access to any computer to be an offence. This crime consists of two ingredients: '*actus reus*' that is represented by access to any computer and '*mens rea*,' which occurs when the access is being intentional and unauthorised.

The *actus reus* of this crime requires that the criminal gains access to the computer and causes the computer to accomplish any function, such as switching on the computer or deleting data or programs that are held therein. This means that the accused to be guilty of hacking according to section 1 should have physical interaction with a computer. However, if the accused has no physical interaction with the computer, such as reading of confidential computer output, or reading displayed information on screen he may not be guilty of a hacking crime within the scope of section 1 of the Act.[59] The *actus reus* of the crime takes place, even if the criminal does not actually obtain access to the data or programs within the computer or successfully subvert the security measures in

[58] Memorandum from the Society for Computers and Law—'Internet Interest Group and Privacy and Data Protection Interest Group paragraph' 5 available at <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/7012402.htm> viewed on 25 March 2012; Home Office, 'Identity Fraud Steering Committee' available at <http://www.identity-theft.org.uk/definition.htm> accessed on 25 March 2012

[59] M Wasik, 'The Computer Misuse Act 1990' Vol. (1990) Criminal Law Review 767-779

place.[60]

The Computer Misuse Act 1990 does not define the term 'any computer' and that causes a deep argument among judges as well as scholars. The argument is divided into two groups. The first group[61] believes that section 1 applies only when there is unauthorised access from one computer to another. It cannot be applied if the unauthorised access has been committed from the same computer or the criminal bought key-cutting equipment to gain unauthorised access to the computer's location and make it perform any function mentioned. For instance, in *R v Cropp*[62], Judge Aglionby at Snaresbrook Crown Court stated that the accused did not commit an offence because the Computer Misuse Act 1990 only governs hackers who use one computer to gain access to another whereas in this case only one computer was used. However, Lord Taylor CJ in the Court of Appeal disagreed with that and rejected the accused's defence stating that the term 'any computer' in s. 1 should have its ordinary meaning. He pointed out that:

> [I]n our judgment there are no grounds whatsoever for implying, or importing the words "other" between "any" and "computer", or excepting the computer which is actually used by the offender from the phrase "any computer".

However, the Court of Appeal did not overturn the judgement of the lower court, thereby leaving some uncertainly as to the meaning of the Computer Misuse Act 1990 on this point.

On the other hand, the second group[63] pointed out that it would be important if the

---

[60] M Wasik, supra, note 59

[61] S Singleton, 'Comment Computer Misuse Act 1990-Recent Developments' (1993), Vol. 57 Journal Criminal Law 181-183; Daithí Mac Síthigh, in his comments on the conviction related to *Ellis v DPP* {[2001] EWHC Admin}, stated that section 1 is potentially quite broad, but he implicitly agreed with the court's opinion when he stated that, although the issue has not been directly discussed by the court. However, some scholars have pointed out that there should be at least a proper notice in place in order for access to be considered unauthorised. In this case the accused used university computers (which had been left logged on by authorised users) Daithí Mac Síthigh, 'Law in the last Mile: Sharing Internet Access Through WiFi' 2009 Vol. 6 (2) Scripted 364 available at <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-2/macsithigh.pdf> viewed on 15 July 2012

[62] *R v Cropp* 05/07/1991/[1991] 7 CLSR 168, [1991] CL&P; [1992] 3 WLR 432

[63] S Fafinski and N Misassian, 'UK Cybercrime Report 2009' 2009, 28 available at <http://zunia.org/uploads/media/knowledge/613-GRLK_PRD1256978512.pdf> viewed on 10 March 2012; K Stein, '"Unauthorised Access" and the U.K. Computer Misuse Act 1990: House of Lords "leaves no room" for ambiguity' (2000) Vol. 6 (3) Computer and Telecommunications Law Review 63-66; All Party Internet Group, '"Revisions of the Computer Misuse Act': Report of an Inquiry by the All Party Internet Group" 2004 available at <http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry/CMAReportFinalVersion1.pdf> accessed on 3 October 2011

legislature does not define some terms, which are mentioned in the Computer Misuse Act 1990 and leave them to be as broad as possible in order to cover all types of illegal activities that may happen in future and to ensure the law keep up with technological developments.

The term of unauthorised access may also give rise to difficulties when a judge applies the Computer Misuse Act to crimes of unauthorised access, particularly, if the unauthorised access is combined with authorised access. Although the UK legislature in section 17(5)[64] determines the meaning of the term unauthorised access, the UK judge may find it difficult to prosecute a person who has accessed another person's computer and made the computer achieve its function, such as copying stolen information held in it, because in this example there is no unauthorised access. In addition, the application of section 1 may lead to contrasting in judgments and different interpretations as to the meaning of to the term unauthorised access.

In *R v Bignell*,[65] for example, the Divisional Court held that the accused's conduct was authorised whereas in *DPP v Lennon*[66] the High Court held that the accused's conduct was unauthorised.

The *Bignell* judgment raised debate between scholars and judges.[67] For instance, when

[64] Section 17(5) of the Computer Misuse Act 1990: (a)ccess of any kind by any person to any program or data held in a computer is unauthorised if—(a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled'.

[65] *R v Bignell* 1997 [1998] 1 Cr. App. R. 1, in this case two police officers instructed computer operators to obtain information from the Police National Computer to use it in their favour and not for official purposes. The Commissioner had previously ruled that police computer should be used to the police purposes only. The accused knew this rule. The judge stated that Computer Misuse Act has come to protect the integrity of the computer rather than the information stored in it, and consequently, there was no unauthorised access. The Division Court upheld this judgment; *R v Raphael Gray*, Swansea Crown Court 2001; contrary to these cases, the All Party Internet Group stated that we accept some legal opinion, but we believe that there are no practical problems with respect to unauthorised access to computer program or data. They stated that the Act could be applied to both, irrespective of whether the access is authorised or unauthorised; All Party Internet Group, supra, note 63 at 40

[66] *DPP v Lennon* [2006] EWHC 1201, in this case, a disgruntled employee who has recently been dismissed from the company, sent bombardment emails to a company machine. The trial court stated that the machine is already was designed to receive and respond to such emails, thus, the accused conduct was authorised and there is no case to answer. However, the Divisional Court remitted the case back to the trial court on the basis that it had wrongly decided that there was no case answer. As a result, the accused ruled according to Computer Misuse Act and he ultimately pleaded guilty.

[67] Sumroy stated following a decision like this means there is no a crime under section 2 and 3 of the Act, if this correct, highlights the gaping loophole that remains in this area of the law. Disgruntled or opportunistic employees with authority to access a computer may exploit that authority and access that computer to use or modify the information held on it for an unauthorised purpose, R Sumroy 'Computers:

their Lordships in the House of Lords discussed the case in *R. v Bow Street Magistrates' Court Ex p. Allison*[68] they found that the Division Court posed the wrong question. They stated that it should have focused on whether the accused had authority to access the actual data involved, not only over the data in question. However, they stated that the decision was 'probably right'. They mentioned many reasons to justify their conclusion. One of these reasons was stated by Lord Hobhouse who pointed out that the accused in *Bignell* had authority to access the data, which were secured by the computer operators, as they were authorised to access a National Police Computer. The computer operators were responding to police officers' requests. As a result, the access to the data was authorised.

The debate that was raised with respect of the *Bignell's* judgment stressed that there is a gap in the Computer Misuse Act 1990, which remains unresolved. McEwan[69] observes that the judgment in the case of *Lennon* determined this gap and illustrated the inadequacy of the Computer Misuse Act. This inadequacy appears when the Computer Misuse Act 1990 comes to governing the misuse that may occur on the part of an authorised person. From the two contrasting judgments in *Lennon and Bignell*, it seems that the judges distinguished between two types of the misuse: the misuse on the part of the authorised person and that, which has been requested, from an authorised person by another person who is unauthorised to access the computer programme or data.[70]

The *mens rea* of a hacking crime is represented by unauthorised access to any computer. A person or an accused should know that he has no authority to access to secure access to any program or data within that computer, and he accesses it.[71] He should also have an intention to access a computer without any further intention to carry out any other act.[72] It is not necessary to have intent to be directed at any specific program or data, or program or data of a particular kind, or that it has been held in a

---

Computer Misuse and Data Protection' (1997) Vol. 3 (5) Computer and Telecommunications Law Review T119-120; C Gringras, 'To Be Great Is to Be Misunderstood: the Computer Misuse Act 1990' (1997) Vol. 3 (5) Computer and Telecommunications Law Review 213-215

[68] [2000] 2 AC 216

[69] N MacEwan, 'The Computer Misuse Act 1990: Lessons from its Past and Prediction to Its Future' (2008) Vol. 12 Criminal Law Review 955-967

[70] ibid

[71] ibid; C Gringras, supra, note 67

[72] A Nehaluddin, 'Hacker's Criminal Behaviour and Laws Related to Hacking' (2009) Vol. 15(7) Computer and Telecommunications Law Review 159-165

particular computer. Regarding unauthorised access, section 1 does not distinguish between the people who access another computer as an amateur or those who have been recruited by other people who have more sinister motives.[73]

Some scholars[74] take the view that section 1 is too broad and has applications, which may extend beyond the UK's boundaries. It has also been pointed out section 1 deals with hacking offences, which may be covered by sections 2 and 3 of the Act[75], thereby rendering section 1 to be pointless in this context.[76] In addition, a dissenting argument[77] stated that section 1 is inadequate in the legislation to combat complicated misuse, such as outside hacking that may be committed against a computer and it is a weapon against insider hackers only.

The conclusion of the previous analysis is that the UK legislature intends in section 1 to criminalise unauthorised access to people's computers by hackers only. It does not determine a specific data or program to be a subject of this unauthorised access. It seems that section 1 of the Computer Misuse Act 1990 protects the integrity of people's computers[78], rather than their identities. If the legislature intends to protect a person's means of identification, it should determine the type of information as a subject of unauthorised access.

In addition, section 1 prevents hackers only from getting access to people's computers. However, the hacking is but one method of many methods that can be used by criminals to obtain people's identities. Most methods that may be used to commit identity theft remain unpunishable under this section. Consequently, this section on its own is

---

[73] D Ormerod, *Smith and Hogan's Criminal law* (13th edn Oxford University Press 2011) 1048

[74] S Singleton, supra, note 59; P Ryan and A Habirson, 'The Law on Computer Fraud in Ireland-Development of the Law and Dishonesty' (2009) 10 available at <http://www.arthurcox.com/uploadedFiles/Publications/Publication_List/Arthur%20Cox%20-%20The%20Law%20on%20Computer%20Fraud%20in%20Ireland,%20June%202010.pdf> viewed on 8 February 2012; Daithí Mac Síthigh, supra, note 61

[75] A Nehaluddin, supra, note 72

[76] B Evans, 'Computer: Hacker How Best to Solve It', 15 July 2008 lawdit readingroom available at <http://www.lawdit.co.uk/reading_room/room/view_article.asp?name=../articles/5167-Computer-Hacking-How-Best-To-Solve-It.ht> viewed on 2 October 2011

[77] S Singleton, supra, note 61, 2

[78] English Commission Law no. 186, Criminal Law, Computer Misuse 1989, Paragraph 2.11-2.15, 11-12; MacEwan stated that there was an argument about whether the law should directly address the issue of *information theft* before the Computer Misuse Act 1990 had come enforce and continue. Therefore, the notion that the law should be discussed the concept of *information* rather than the computer integrity of its security. Moreover, he pointed out that the Computer Misuse Act 1990 offered the simplest way to reform the law. N MacEwan, supra, note 69

inadequate to govern identity theft. As a result, when the Iraqi legislature intends to enact a comprehensive Act it cannot adopt or borrow its provisions to combat identity theft. In spite of the previous flaw of section one, its provisions can assist the Iraqi legislature if it intends to legislate a new Act to protect computers that are connected with the internet, particularly become Iraq has no specific law that can be used to deal with crimes that are committed against computers and internet.

6.1.4.2 How Relevant Is Section 2 of the Computer Misuse Act 1990 to Iraqi Situation?

In section (2) of the Computer Misuse Act 1990, a person may be guilty of an offence if he or she obtains unauthorised access to another person's computer with intent to commit or facilitate further crimes, such as fraud or access to another person's means of identification.[79] This crime consists of two elements *actus reus* and *mens rea*.

The *actus reus* of the offence (as stated in section 2 of the Computer Misuse Act 1990) occurs if the criminal without authority accesses another person's computer and commits other crimes or facilitates them. The commission of the offences that hackers intend to commit or facilitate through unauthorised access may take place at the same time that the unauthorised access happens, or they may be take place later.[80]

The *mens rea* of the offence of unauthorised access (to commit other crimes or facilitate them) occurs when the hacker knows that he has no authority to access another person's computer. He should also have an intention to commit further crimes or to facilitate them, even if those crimes are impossible.[81] The *mens rea* of this offence is the 'ulterior intent'. Recklessness is not enough to prove the *mens rea* of this offence.[82]

The main advantage of section 2 of the Computer Misuse Act 1990 is that it deals with a specific crime. It governs every unauthorised access to a computer with intent to commit or to facilitate other crimes. Identity theft is one of the crimes that criminals

[79] *R (McKinnon) v Secretary of State for Home Affair* [2009] EWHC 2021 (Admin)
[80] S 2(3) Computer Misuse Act 1990
[81] Wasik, supra, note 59
[82] *Zezev and Yarimaka v the Governor of HM Prison Brixton and the Government of the United States of America* [2002] EWHCA 589 (Admin); D Ormerod, *Smith and Hogan's Criminal Law* (12th edn, Oxford University Press Oxford New York 2008), 1017

sometimes intend to gain unauthorised access to commit it.[83] Accordingly, the accused can be subject to the criminal liability that this section attends.[84] As it was discussed in chapter three, criminals use some sophisticated, such as hacking, phishing, spamming, or spoofing to obtain a person's means of identification. Methods like those sometimes enable criminals to gain unauthorised access to another person's computer. However, criminals who have authorised access may use phishing, spamming or spoofing to obtain a person's means of identification. Criminals also use traditional methods to obtain the person's means of identification, thus they may not be subject to the criminal liability under this section. As a result, it is inadequate to govern comprehensively identity theft and courts still need a comprehensive law to combat identity theft.

Turning now to the question that was asked in the beginning of this section: whether the Iraqi legislation can espouse or borrow provisions from this Act, it might be said that this section is inadequate for the Iraqi legislature as a solution to combat identity theft for the reasons mentioned above. In addition, it suffers from the same problems that section 1 of this act suffers from.[85] Moreover, it seems that this section can protect a person's means of identification or information held on a computer when there is unauthorised access only. However, it cannot be applied to a person who obtains another person's information, such as his means of identification held on a computer, through *authorised access* with intent to use it in fraudulent activities.[86] Nevertheless, as stated with respect to section 1, the Iraqi legislature can benefit from provisions that are mentioned in section 2 when it intends to criminalise the illegal methods, such as

[83] See in the same meaning Warren B. Chik, 'Challenges to Criminal Law Making in the New Global Information Society: A Critical Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore' footnote 57 available at<www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc> accessed on 15 July 2012

[84] R Walton, 'The Computer Misuse Act' (2006) Vo. 1 (1) Information Security Technological Report 39-45; the judge Wight in his comment on Zezev case stated that a person may be guilty of unauthorised access if he by misusing or bypassing any relevant password, places in the files of the computer a bogus e-mail by pretending that the password holder is the author when he is not, then such an addition to such data is plainly unauthorised, as defined in section 17(8); intent to modify the contents of the computer as defined in section 3(2) is self-evident and, by so doing, the reliability of the data in the computer is impaired within the meaning of section 3(2)(c)

[85] The first problem that it caused a deep argument among judges as well as scholars is in section 1 of the Computer Misuse Act the UK legislature does not define or determine the term "any computer", which has led to different judgments and views. it also does not define the term "unauthorised access" this caused a difficulty for judges when they tried to apply the Computer Misuse Act to the crimes that have been committed by unauthorised access, which is combined with authorised access. Section 1 of the Computer Misuse Act 1990 is described as too broad and that may cause a problem when section 2 is applied to the crimes that are covered by section 1.

[86] *R. v Bow Street Magistrates' Court Ex p. Allison*, supra, note 68

hacking that are used to obtain a person's means of identification.

6.1.4.3 Does It Fit the Purpose: Section 3 of Computer Misuse Act 1999 and the Potential Iraqi Identity Theft Legislation?

According to section 3 of the Computer Misuse Act 1990, a person may be guilty of an offence if he or she accesses another person's computer without authority with the intention to modify the contents, such as programs or data that have held therein. For instance, the person may be guilty of an offence according to this section if he adds, or deletes, programs or data held in another person's computers.

The *actus reus* of the crime under section 3 takes place when a person impairs the operation of the computer, prevents, or hampers access to a program or data by the legitimate user. In addition, it may involve altering or erasing any program or data on the computer. It also occurs when other programs, such as viruses may also be added to the computer. The *mens rea* of the crime is mentioned in this section takes place if a person knows that he or she is modifying the contents of the computer without authority, or affecting the reliability of programs or data.[87]

To scrutinise whether section 3 of the Computer Misuse Act 1990, the author should compare the elements of identity theft with the above elements of the crime. The first thing that may come to mind is that offline identity theft offence cannot be subject to this section or to any section of the Computer Misuse Act 1990. The second thing is that the *actus reus* of identity theft, as was shown in chapter three[88], takes place when the accused uses sophisticated or non-sophisticated methods to obtain, transfers, or uses another person's means of identification. However, the *actus reus* of the crime that is stated in section 3 of 1990 Act takes place when the accused impairs, prevents, or hampers the legitimate user to access to a program or data that held in a computer. There is no obtaining, transferring, or using of data or programs. The data or programs remain with user of the computer.

---

[87] *Zezev and Yarimaka v. the Governor of HM Prison Brixton and the Government of the United States of America* , supra, note 82

[88] Identity thieves may use several methods to obtain people's means of identification. They may steal people's wallets or purposes; steal their mail or use spam or phishing to get this information. According to the US identity theft laws, the transfer, or the use of, a person's means of identification is considered the *actus reus* of identity theft.

The *mens rea* of identity theft takes place when the accused uses another person's means of identification as his own identification to get benefits or to achieve illegal purposes in the name of that person, whereas the accused of the crime that is mentioned in section 3 of Computer Misuse Act 1990 has no intention to use another person's means of identification to get benefits or achieves illegal purposes. The accused under section 3 intends to impair the computer of the user or to prevent him from using his computer properly.

It appears that section 3 of the Computer Misuse Act 1990 does not cover the unlawful obtaining of a person's means of identification. It protects the integrity of computers only. However, it has been analysed in this section to complete the investigation of the Computer Misuse Act 1990 in order to scrutinise whether its provisions can be adopted or borrowed by the Iraqi legislature to enact a new Iraqi Act to deal with identity theft. The Iraqi legislature can adopt or borrow the provisions of section 3 if it intends to enact a new law to prevent the misuse of computers and internet.

6.1.4.4 Conclusion

In sum, it could be said that every a new Act has opponents and supporters. The All Party Internet Group[89] is one of the supporters of the Computer Misuse Act. Its report entitled 'Revision of the Computer Misuse Act,' has gone against the view that this Act is inadequate to govern all sophisticated methods that are used to commit *identity theft* and suggests that the Computer Misuse Act 1990 is necessary to plug the gap in the traditional theft provisions. The report stated that this Act could cover all types of malicious programs, such as spyware, spam and others.[90]

Contrary to the All Party Internet Group's view, the English Law Commission pointed out in its paper number 186 that the main argument in favour of a hacking crime springs from the need to protect the integrity and security of computer systems from attacks by unauthorised persons who enter those systems, rather than the need to protect the information. The integrity and security of the data are protected from those

[89] All Party Internet Group, supra, note, 63, 6
[90] ibid; S Fafinski and N Misassian, supra, note 63

unauthorised persons irrespective of their intention or motive.[91]

In addition, in his comments on Computer Misuse Act 1990, Charleworth[92] stated that:

> [T]his rather piecemeal process of legislation has led to claims that the Act is no longer (or indeed never was) capable of achieving the purpose for which its originators intended it, namely the control of computer hacking.

The emergence of the internet has also demonstrated that the Computer Misuse Act 1990 is inadequate when it comes to dealing with the hacking that is remotely committed via the internet.[93] For example, at the request of the Attorney-General whether the Computer Misuse Act can be applied to the hacking at all, the Court of Appeal stated that it is difficult to apply the Act to 'remote hacking.'[94] Therefore, this issue should be caught in the legislative net- through further legislation.[95]

However, it is stated that it is better for legislation to address criminal intent and to retain definitions as broad as possible to ensure the law keep up with technological developments.[96] For instance, Walton[97] stated that the computer and network technology enable hackers to act remotely over a computer network. This ability to hack into computers remotely makes challenges for traditional notions of legal jurisdiction, but the Computer Misuse Act 1990 can overcome these challenges because it is drafted in a manner can govern them. Conversely, Christian stated that 'as the Bedworth case[98] has shown, this Act -- intended to close the loopholes in earlier

---

[91] English Law Commission no. 186, Criminal Law, Computer Misuse 1989 Paragraph 2.11-2.15, 11-12; N MacEwan, supra, note 69

[92] A Charlesworth, 'Legislating Against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990' (1993) Vol. 4 (1) Journal Law & Information Science 80-93

[93] K Stein, supra, note 63

[94] Attorney General's Reference, (No. 1 of 1991) [1993] Q B 94

[95] MacEwan, supra, note 69

[96] K Stein, supra, note 63, 5; Walton stated that it is impossible to predict in detail all the uses and abuse of technology that may happen for more than a very short period ahead because computer technology is changing rapidly. The drafters of the CMA were well aware of that and were concerned to ensure that the act was proof against future technology change. The most obvious example is the definition of a computer. The legislatures have not defined the term of computer. The legislatures allow the courts to interpret the computer term in manner that keeps up the law with technology development. Walton, supra, note 82

[97] ibid, 40

[98] The facts in this case are as follows: on June 26th 1991, the police mounted "Operation Killern" from four different forces. Bedworth and his two co-defendants were members of a hacking group called Eight Legged Groove Machine (8LGM). The defendants were arrested at their home addresses at around midnight. The prosecution alleged that all three were arrested in the act of committing an offence. In the police raid on the defendants' homes, Computer equipment and documentation were seized.

legislation -- is now itself shown to be deeply flawed.'[99]

It might be said that UK courts cannot rely upon the Computer Misuse Act 1990 to protect personal information and the avoidance of such information being taking in identity theft scams, or other sophisticated methods. The UK courts cannot rely upon Computer Misuse Act 1990 because it has been enacted to protect the integrity of computers.[100]

Having analysed all UK laws, such as the Data Protection Act 1998, Theft Act 1968, Fraud Act, and Computer Misuse Act 1990, it is evident that these Acts are inadequate to combat identity theft. It might be said that the Iraqi legislature could not adopt or borrow provisions from UK laws to enact a comprehensive Act to govern identity theft and fill in the gap in its existing theft offence laws and Information Crimes Project 2011. Moreover, even in the UK courts decisions that deal with the misuse of a person's means of identification, the situation is still ambiguous and cannot assist the Iraqi legislature to draw an adequate legal framework to govern identity theft. However, as was stated previously, these laws cannot be utterly abandoned. The Iraqi legislature could adopt or borrow provisions from these laws to enact a new Act in order to protect the integrity of computers, as well as amend fraud laws, rather than the protection of a person's identity *per se*. Such measures will help support the construction of a legal framework to combat some of the activities that lead to identity theft in Iraq.

Bedworth and his co-defendants were charged with conspiracy to commit offences contrary to section 3 of the Computer Misuse Act 1990. The prosecution alleged that three defendants had gained unauthorised access to the computer systems of academic, government and commercial organisations and modified the systems to which they gained access. They were also charged with conspiracy to make dishonest use of services provided by British Telecom. The prosecution accepted that Bedworth and his two co-defendants did not hack into computers for gain or for any other criminal purpose. The defendants had never actually met, but they had communicated via electronic bulletin boards. The three defendants were charged with related to five institutions: Brighton Polytechnic, Bristol Polytechnic, and the European Organisation for the Research and Treatment of Cancer (EORTC) in Belgium, the European Economic Community in Luxembourg, and the Financial Times. At the trial, it was alleged that Bedworth had made changes to the code of a share index database at the Financial Times which cost £25 000 to repair. In addition, it was alleged that he had disrupted important research work by overloading the EORTC's computer and left the organisation with a £10 000 phone bill.
At the end of the trail, Bedworth's co-defendants pleaded guilty to the conspiracy charge under s3 of the Computer Misuse Act 1990 and to the charge of conspiring to obtain unlawfully telegraphic services, but Bedworth pleaded not guilty. Bedworth alleged that he was addicted to computer use and by virtue of that addiction was unable to form the necessary intent. After hearing for an expert witness, the court acquitted Bedworth. This case is not published.

[99] C Christian, 'Down and Out in Cyberspace' (1993) 90 L S Gaz. 2

[100] Daithí Mac Síthigh, supra, note 61, 366

As a result of the above criticisms against the adequacy of UK laws to govern identity theft, the study in the next section will examine US identity theft laws to scrutinise whether the Iraqi legislature can adopt or borrow provisions from the USA' laws to enact a comprehensive Act to govern identity theft.

6.1 Adopting or Borrowing Provisions from US's Laws to Combat Identity Theft

In this section, the author will assess whether the Iraqi legislature can borrow or adopt from US identity theft laws the three elements needed to criminalise the unlawful obtaining of another person's means of identification, and then use it to commit other crimes or achieve illegal purposes.

US theft laws failed to protect a person's means of identification from the act of the illegal obtaining, and then using it to commit other crimes. The US courts were also not able to overcome this inadequacy in US theft offence laws. The US legislature therefore enacted new laws that describe identity theft as a crime, to protect a person's means of identification: the Identity Theft and Assumption Deterrence Act 1998, [101] (referred to 'Identity Theft Act') and the Identity Theft Penalty Enhancement Act 2004.[102] Provisions of these laws specifically deal with the identity theft phenomenon by prohibiting the transferring, usage and possession of another person's means of identification and his financial information. This poses the question whether such laws are properly framed and are a measured response to this new criminal phenomenon, or whether they are overly broad and inadequate to be adopted by the Iraqi legislature. In order to answer the above questions, the provisions of these two laws will be analysed below.

6.2.1 Definition of Identity Theft

In section 1028 (a)(7) of the Identity Theft Act 1998[103], the legislature defines identity theft as

[101] Identity Theft and Assumption Deterrence Act 1998, Pub. L. 105-318, 18 §1028 October 30, 1998, 112 stat. 3007
[102] Identity Theft Penalty Enhancement Act 2004 Sec. 2 Aggravated Identity Theft, Pub. L. 108-275, 18 §1028a (1) July 15, 2004, 118 Stat. 831
[103] Identity Theft and Assumption Deterrence Act 1998 supra

> [W]hoever, in a circumstance described in subsection (c) of this section: knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet in any unlawful activity that constitutes a violation of Federal law or that constitutes a felony under any applicable State or local law.

The US legislature enacted the Identity Theft Penalty Enhancement Act 2004 to underpin the Identity Theft Act of 1998. Therefore, the same definition of identity theft can also be found in the Identity Theft Penalty Enhancement Act 2004.[104] The Identity Theft Penalty Enhancement Act 2004 increases the punishment for identity theft when the stolen means of identification is used to commit other crimes, such as terrorist crimes. The crime that is stated in this Act is called aggravated identity theft. In effect, it might be said that the crime that is stated in the Identity Theft Penalty Enhancement Act 2004 is not considered a subset of identity theft that is contained in the Identity Theft Act 1998 because the courts in the US sometimes rule that the accused on both the original identity theft and the stated crime in the Identity Theft Penalty Enhancement Act 2004.

The previous definition determines the main ingredients of identity theft, *mens rea* and *actus reus*. The merits and demerits of this definition may not appear unless the ingredients *actus reus* and *mens rea* are examined. Thus, in the next two sections these two elements will be examined.

6.2.2 *Actus Reus* of Identity Theft in US Identity Theft Laws

According to the Identity Theft and Assumption Deterrence Act 1998, the *actus reus* of identity theft consists of three elements: illegal act, means of identification and belonging to another person.

The core behaviour that is prohibited by the Identity Theft Act of 1998 is the illegal transferring of or using a means of identification of another person, such as his name, address, mother's maiden name, or his social security number to commit other crimes, such as fraud or terrorism. The US legislature in the Theft Penalty Enhancement Code 2004, added a new prohibited element to the elements of the *actus reus* of identity theft, by providing that identity theft takes place when a person, during or in relation to any

[104] Identity Theft Penalty Enhancement Act 2004 supra

felony violation enumerated in subsection (c)[105] transfers, possesses or uses a means of identification of another person. It appears from the definition that set forth in the 2004 Act the term 'possession' is the prohibited element that is added to the elements of the *actus reus* of identity theft.[106] The question remains: can the Iraqi legislature borrow or adopt the stated elements of the *actus reus* of US identity theft laws when formulating a new Act for Iraq.

6.2.2.1 Borrowing or Adopting the Elements of the *Actus Reus*

As stated in the Introduction chapter, there is a difference between identity theft as a crime and its effects (or so called the use of the stolen identity as a means to commit other crimes). Identity theft takes place when the criminal takes or acquires another person's means of identification, and not when this means of identification is transferred or used to commit other crimes. It might be argued that using the terms 'transferring', and 'using', is an inadequate basis for the criminalisation of the act of the unlawful obtaining of another person's means of identification. It is an inadequate basis for the criminalisation because it does not deal with the procedures or methods that are used to commit identity theft.[107] The terms *transferring* and *using* do not amount to the actual occurrence of identity theft[108] because it has already taken place at this point.

---

[105] Section (c) of the Identity Theft Penalty Enhancement Act 2004 states: definition.—For purposes of this section, the term 'felony violation enumerated in subsection (c)' means any offense that is a felony violation of—''(1) section 641 (relating to theft of public money, property, or rewards), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), or section 664 (relating to theft from employee benefit plans); ''(2) section 911 (relating to false personation of citizenship); ''(3) section 922(a)(6) (relating to false statements in connection with the acquisition of a firearm); ''(4) any provision contained in this chapter (relating to fraud and false statements), other than this section or section 1028(a)(7); ''(5) any provision contained in chapter 63 (relating to mail, bank, and wire fraud); ''(6) any provision contained in chapter 69 (relating to nationality and citizenship); ''(7) any provision contained in chapter 75 (relating to passports and visas); ''(8) section 523 of the Gramm-Leach-Bliley Act (15 U.S.C.6823) (relating to obtaining customer information by false pretenses "pretences"); ''(9) section 243 or 266 of the Immigration and Nationality Act (8 U.S.C. 1253 and 1306) (relating to wilfully "wilfully" failing to leave the United States after deportation and creating a counterfeit alien registration card); ''(10) any provision contained in chapter 8 of title II of the Immigration and Nationality Act (8 U.S.C. 1321 et seq.) (relating to various immigration offenses); or ''(11) section 208, 811, 1107(b), 1128B (a), or 1632 of the Social Security Act (42 U.S.C. 408, 1011, 1307(b), 1320a–7b (a), and 1383a) (relating to false statements relating to programs under the Act).''

[106] The term possession has been added to the Identity Theft and Assumption Deterrence Act 1998 when Congress amended section 1028a (7) on January 7, 2004 by 108th Congress-second session convening.

[107] A Steel, supra, note 48, 510; Nicole M Buba, 'Wagin War Against Identity Theft: Should the United States Borrow from the European's Union Battalion? (1999-2000) 23 Suffolk Transnat'l L. Rev. 633 -665

[108] M Gercke, 'Project on Cybercrime, Internet-related Identity Theft' A Report has been Prepared within the Framework of the Project on Cybercrime of the Council of Europe as a Contribution to the Conference "Identity fraud and theft – the logistics of organised crime" (2013) available at

Both the terms 'transferring' and the 'use' are aftermath illegal activities that carry out the impetus of the criminal to commit other crimes. The use of, or transferring of, another person's means of identification is a term used as a preparatory act to commit other crimes.

Moreover, the criminalisation of the use of or transferring the means of identification causes a problem that prevents the principal actor to be guilty of identity theft because when the US legislature enacted the Theft Act 1998 it failed to properly describe the behaviour needed to criminalise it. Fundamentally, the transferring, or the use of, another person's means of identification are often described as identity theft, whereas identity theft has been committed at an earlier point, *prior to* the transferring, or the use of, another person's identification without consent to commit other crimes.[109] For example, if someone steals a car belonging to another person, and then uses it to commit another crime, the latter is a crime committed by using a stolen means, which in this case is represented by the car.

De facto, it seems that the US legislature by enactment of this Act intended to criminalise the act of unlawful obtaining of another person's means of identification, but it failed to do so. It criminalised the use of the means of identification of another person rather than the stealing of such identification in the first glance.[110] Criminalising the element 'transfer of or use of' to commit other crimes may be ineffectual and inadequate to fight identity theft. Identity theft may be fought as some scholars and professionals[111] suggest, by criminalising the earlier acquisition of another person's

---

<http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf> accessed on 22 May 2013

[109] Kristen S Provenza, 'Identity Theft: Prevention and Liability' (1999) Vol. 3 North Carolina Banking Institute 319-336; In section 480.4 of the Commonwealth Criminal Code that deals with financial information, The legislature stated that (a) person is guilty of an offence if the person: (a) dishonestly obtains, or deals in, personal financial information; and
(b) obtains, or deals in, that information without the consent of the person to whom the information relates; contrary to the US legislature, the Canadian legislature in 402.2 (1) of the Criminal Code of Canada stated that "(e)veryone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence". See also the Queensland Criminal Act of 1899 s 408D (1) ins 2007 No. 14 s16 and amended in 2010 s 1 (4)

[110] *United States v. Godin*, 534 F.3d 51 (1st Cir. 2008)

[111] Lauren L Sullins, 'Phishing for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft' (2006) Vol.20 (1) Emory International Law Review 397-434; R August, 'International Cyber-Jurisdiction: A Comparative Analysis' (2002) Vol. 39 American Business Law Journal 531-573; Press Release, 'New Leahy Bill Targets "Phishing" and "Pharming"' Senator Patrick

identification rather than focusing penal effort against the subsequent transfer of, or use of, it in fraudulent or other unlawful activities. Transfer (as an element of identity theft) also gives rise to the problem that if the victim voluntary submits his means of identification to the offender, is the offender guilty of identity theft. The answer will be negative because there is no 'transferring' of another person's means of identification. Both the Identity Theft Act 1998 and the Identity Theft Penalty Enhancement Act 2004 do not cover this issue.[112]

It could be said that the Iraqi legislature should by looking to the above US legislation for guidance criminalise the obtaining of another person's means of identification with intent to commit other crimes. In addition, it can borrow or adopt the provisions that criminalise the transferring or the use of this means to commit other crimes because the illegal transferring or the use of another person's means of identification is considered a dangerous act that may facilitate the commission of other crimes. However, what the United States legislation does not provide guidance on is the provision of suitable provisions for prohibiting identity theft *per se*.

6.2.2.2 The Criminalisation of Sophisticated Methods to Commit Identity Theft

Sophisticated methods (discussed in chapter three), may be used by criminals to obtain a person's means of identification are considered as dangerous as transferring or using another person's means of identification. These methods need more attention from the US legislature in order to deter and prevent traditional crimes.[113] It seems that the US legislature in the Theft Act of 1998 and the Identity Theft Penalty Enhancement Act 2004 has failed to criminalise some of these sophisticated methods, such as spam, phishing, or spoofing, which may stand alone as crimes.[114] Senator Leahy[115] considered that the criminalisation of sophisticated methods is as important to prevent serious

---

Leahy, Speech on the Senate Floor on the Introduction of the "Anti-Phishing Act of 2005" (Feb. 28, 2005) [hereinafter Leahy Speech] available at <http://www.senate.gov/galleries/daily/224pr05.html#anchor334628> accessed on 12 July 2012; A Ramasastry, 'The Anti-Phishing Act of 2004: A Useful Tool Against Identity Theft' 2004 available at <http://writ.news.findlaw.com/ramasastry/20040816.html> accessed on 22 March 2012

[112] M Gercke, supra, note 108

[113] Warren B Chik, supra, note 83

[114] Anti-Phishing Act of 2004, S. 2636, 108th Cong. § 1351 (2004)

[115] Senator Leahy, 'Statement, Introduction of the "Anti-Phishing Act Of 2004"' 150 Cong, Rec. S7897 (July 9, 2004) [hereinafter Senator Leahy Statement] (statement of Sen. Leahy) available at <http://www.gpo.gov/fdsys/pkg/CREC-2004-07-09/pdf/CREC-2004-07-09PgS7897-2.pdf> viewed on 12 July 2012

crimes that may cause great damage for individuals. In effect, identity theft is not considered a primary aim of the criminal; rather, it is committed to facilitate other crimes, such as computer fraud.[116] The criminal may use computers to create a bogus website resembling a legitimate website in order to convince individuals into providing their personal or financial information, such as credit card details.

In the US, criminals who use stolen identity to commit online crimes, such as fraud may be subject to a charge under more than one statute, such as the Credit Card Fraud Act, the Computer Fraud Act and other laws. In a recent case[117], for instance, the US Justice Department applied the Credit Card Fraud Act instead of the Identity Theft Act 1998 to prosecute an accused who used phishing to steal another person's information, although the Identity Theft Act would have been more appropriate.[118] This issue -which Act to use- confuses courts and the accused, because they do not know exactly which law can be applied to the illegal activity that is committed.[119]

It could be argued that to solve the above problem that the Iraqi legislature should set out a specific part in a new potential identity theft Act, to contain provisions that criminalise some sophisticated methods as stand-alone as crimes. They should also criminalise creation of a false website (which is designed to look like a legitimate one) used to commit identity theft by inducing individuals into divulging their personal information to the phisher. In addition, the Iraqi legislature should criminalise knowingly sending out emails that may be linked to the website with the intention to commit identity theft.[120] Additionally, it should enact a new Act to deal with computer fraud; particularly as Iraqi legislation contains no Computer Fraud Act or even Computer Misuse Act yet.

---

[116] M Chawki and S Abdel Wahab, 'Identity Theft in Cyberspace: Issues and Solutions' (2006) Vol. 11 (1) Lex Electronica 1-41 available at <http://www.lex-electronica.org/docs/articles_54.pdf> accessed on 13 July 2012

[117] *Criminal Complaint, United States v. Hill* (E.D. Va. May 17, 2004)

[118] Gercke in his comments on the Identity Theft Act 1998 and the Identity Theft Penalty Enhancement Act 2004 stated that the use of phishing to obtain another person means of identification is uncovered by these two laws because the US legislature criminalises the illegal transferring of this means, however, in a phishing case there is no transferring. The victim voluntary submits his means of identification. M Gercke, supra, note 108

[119] Anti-Phishing Act § 1351(a) supra, note 114; A Flanagan, 'The Law and Computer Crime: Reading the Script of Reform' 2005 Vol.13 (1) International Journal of Law & Information Technology 1-15; P Kshirsagar, 'The Problem of Identity Protection in Cyberspace and Some Suggestions' 1-17 available at <http://ssrn.com/abstract=1520204> viewed on 27 May 2012

[120] K S Provenza, supra, note 109, 326

6.2.2.3 Challenges Posed by Criminalising the Possession of Means of Identification

The Identity Theft Penalty Enhancement Act 2004 added a new problem to the aforementioned problems of the *actus reus* of identity theft when it considers the term possession as an ingredient of aggravated identity theft. [121] As Steel observes, the term *possession* as an element of *actus reus* could not be an element of identity theft because a persons' means of identification does not resemble physical or movable property. It cannot be subject to possession by another person. To accuse a person of the unlawful possession of the property, the *actus reus* and *mens rea* should coincide. However, this is unimaginable in the context of the possession of the person's means of identification.[122] For instance, if a person steals another person's means of identification, such as his password or PIN number, and then he is requested to give it away, he may state that he gives the means of identification away, but he may still remember it, and then use it in future. In this case, the *actus reus* and *mens rea* of the crime do not coincide.

In the U.S., the legislature zeal to take steps to protect a person's means of identification or to prevent identity theft in any way in order to protect their economy, thus it criminalised the possession, transferring, and the use of this means of identification. This it was shown and emphasised in some decisions issued by the courts.[123] In these decisions, the courts sometimes exclude the defence of consent to possession, transferring, or the use of another person's means of identification. It might be said that the Iraqi legislature should not consider the 'possession' of means of identification as an element of identity theft. The criminalisation of the sophisticated methods that are used to obtain another person's means of identification, the unlawful obtaining of, transferring, or using it is sufficient to fight identity theft.

---

[121] It is argued that criminalising term possession as an element of identity theft with intent to commit another crime is considered a broad approach. The possession of another person's means of identification means that the accused may use them later to commit other crimes. In fact, US's laws of identity theft require an intention to commit other crimes, thus the use of this means of identification without intent to commit other crimes is not covered by these laws. In addition, it is uncertain whether these laws govern the case of possession of another person's means of identification in which the criminal does not intend to use, but sells them instead. M Gercke, supra, note 108

[122] A Steel, supra, note 48

[123] *United State of America v. Ozuna-Carbrera*, 663 F 3d (1st Cir. 2011), 663 F d 500; *United Sates v. Lumbard*, 706 F.3d 716 C. A. 6 (Mich.) 2013

In conclusion, it might be argued that the above drawbacks in both the Identity Theft Act 1998 and the Identity Theft Penalty Enhancement Act 2004 make them inadequate laws to determine what the *actus reus* of identity theft is precisely. However, these drawbacks do not prevent the Iraqi legislature from borrowing, or adopting the elements "transfer" or "use" of a person's means of identification as elements of the *actus reus* of identity theft if it intends to enact a new identity theft Act. The Iraqi legislature can avoid the drawbacks of the US identity theft laws by criminalising the act of the legal or illegal obtaining of a person's means of identification as well as the transfer, or use of it to commit other crimes. In addition, it should criminalise some methods that may be crimes in themselves.

6.2.2.4 Criminalising Attempted Identity Theft

Although the provisions of attempted identity theft or conspiracy to engage in identity theft commission are not considered elements of identity theft, it is worthy of note that the US Legislature in the Identity Theft Act of 1998 equated the attempt to commit identity theft or conspiracy to engage in identity theft with the commission of substantive crime.[124] It seeks to punish all criminals involved in perpetrating identity theft with the same sanctions that are applied to the principal perpetrator of identity theft. In other words, it equates the criminal who commits a substantive or criminal act with the criminal who commits a preparatory act, such as aiding, or abetting the commission of identity theft.[125] In addition, the US legislature in the Identity Theft Act 1998 has criminalised the use of another person's information with the intent to obtain illegal purposes according to the seriousness of the criminal rather than the seriousness of the act itself.[126] It could be said that even though the Iraqi legislature in the Penal Code of 1969 makes all criminals who are involved in the commission of crimes subject to the same punishment, it would be better if these provisions were included in the new potential law of identity theft.

[124] Identity Theft Act 1998 S 18 U.S.C. § 1028 (c) (C) (E)
[125] 18 U.S.C. §1028 (f) amended by the Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (e) (2003)
[126] A. Steel, supra, note 48

6.2.3 Means of Identification as a Subject of Theft:

The Identity Theft Act of 1998 also defines and determines the term 'means of identification' that constitutes as a subject of theft. It states that a person's means of identification refers to any name or number, such as a name, address, social security number, driver's licence and so on that may be used, alone or combined with other information to identify a specific person.[127] The Identity Theft Penalty Enhancement Act 2004 also adopts this definition with respect to determining the meaning of a person's means of identification. For a means of identification to be a subject of theft, it has to belong to another person. The US legislature in both the Identity Theft Act 1998 and the Identity Theft Penalty Enhancement Act 2004 consider individuals' means of identification as the subject to theft, whereas it omits firms or institutions' identities to be a subject of theft.[128] Currently, the identities of firms or corporations are more susceptible to theft. It might be said the above laws should consider firms or corporations' identities as subject to theft as well.[129]

---

[127] 18 U.S.C. § 1028 (c) (C) (3)

[128] It was stressed in the president identity theft task report that both the Identity Theft Act 1998 and the Identity Theft Penalty Act 2004 do not consider the act of the unlawful obtaining corporates and institutions' identities as identity theft. It was stated in this report that [t]here are two gaps in these statutes, however. First, because both statutes are limited to the illegal use of a means of identification of "a person," it is unclear whether the government can prosecute an identity thief who misuses the means of identification of a corporation or organization, such as the name, logo, trademark, or employer identification number of a legitimate business. This gap means that federal prosecutors cannot use those statutes to charge identity thieves who, for example, create and use counterfeit documents or checks in the name of a corporation, or who engage in phishing schemes that use an organization's name. Second, the enumerated felonies in the aggravated identity theft statute do not include certain crimes that recur in identity theft and fraud cases, such as mail theft, uttering counterfeit securities, tax fraud, and conspiracy to commit certain offenses. 'The President Identity Theft Task: Combating Identity Theft a Strategic Plane' 2007, 65 available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>. However, Congress has not taken this recommendation into account and has not emended these laws. Kristen M. Finklea, 'Identity Theft: Trends and Issues, CRS Report for Congress' 2012, 6 available at <http://www.fas.org/sgp/crs/misc/R40599.pdf> accessed on 23 May 2013

[129] *U. S. v. Hilton,* 701 F.3d 959 C.A. 4 (N. C), 2012; contrast to the United States legislature, The South Australia legislature, in section 144 (A) (a, b) of the Criminal Law Consolidation Act 1935, stated that personal identification information means information relating to a person (whether living or dead, real or fictitious, or an individual or body corporate) that is capable of being used (whether alone or in conjunction with other information) to identify or purportedly identify the person; see also section 408D (7) of the Queensland Criminal Act of 1899 ins 2007 No. 14 s16 and amended in 2010 s 1 (4) *identification information*, of another entity, means information about, or identifying particulars of, the entity that is capable of being used, whether alone or in conjunction with her information, to identify or purportedly identify the entity.
Examples for an entity that is an individual— • information about the individual or the individual's relatives including name, address, date of birth, marital status and similar information • the individual's driver licence or driver licence number • the individual's passport or passport number • anything commonly used by an individual to identify himself or herself, including a digital signature • the

In addition, the Identity Theft Act expands the regulating of stealing personal identification numbers, such as credit card numbers, mobile numbers or account numbers, although such information is governed by the Credit Card Fraud Act as pertaining to access devices,[130] as has been contained by the United States Sentencing Commission.[131] On the other hand, the Identity Theft Act governs many illegal activities that may be autonomously covered by other federal laws.[132]

It could be said that the above definition and determination of a person's means of identification as being subject to theft is considered adequate and that the Iraqi legislature can adopt it after including firms and corporates' identities as a subject of theft. The Iraqi legislature also should consider credit card numbers, mobile numbers or account numbers as a means of identification to protect them from unlawful obtaining, and then using them to commit other crimes, particularly an Iraq has no a specific law to govern both credit card fraud and identity theft. As it was mentioned in chapter three, identity theft consists of two main elements: *actus reus* and *mens rea* and a third element a means of identification or what is referred to as the subject matter of crime.

In the previous two sections, both the US *actus reus* and means of identification have been analysed. The US legislature criminalises the possession, transfer, and use of, a person's means of identification to commit other crimes. However, it failed to criminalise the earlier point of identity theft, which is (the obtaining of this means of identification). In this point, the Iraqi legislature can adopt from the US legislature the terms 'transfer' and 'use' as elements of *actus reus*. The author believes that the term 'possession' should not be an element of *actus reus* of identity theft because the terms transferring and using another person's means of identification include the term

---

individual's financial account numbers, user names and passwords • a series of numbers or letters (or a combination of both) intended for use as a means of personal identification • any data stored or encrypted on the individual's credit or debit card • biometric data relating to the individual • the individual's voice print • a false driver licence or other false form of identification for a fictitious individual. *Examples for an entity that is a body corporate*— • the body corporate's name • the body corporate's ABN • the body corporate's financial account numbers • any data stored or encrypted on a credit or debit card issued to the body corporate.

[130] 18 U.S.C. § 1029 (1) (e) (2003)

[131] United States GAO, 'Identity Theft "Greater Awareness and Use, of Existing are Needed' GAO -02-766, June 2002, 10 available at <http://www.gao.gov/new.items/d02766.pdf> accessed on 25 May 2011

[132] ibid 11

possession even if it is temporary.[133] The Iraqi legislature should add to these elements the illegal act of obtaining of a person's means of identification. With respect to individuals means of identification the US afford an adequate definition of means of identification the Iraqi legislature should adopt it in the potential identity theft Act. However, it failed to criminalise the illegal obtaining, transferring, or using firms' means of identification, thus the Iraqi legislature should consider firms' means of identification as a subject of theft.

6.2.3.1 Belonging to Another Person:

Both the Identity Theft Act 1998 and the Identity Theft Penalty Enhancement Act 2004 do not expressly state this element, but the Identity Theft Act points out that a means of identification refers to (any name or number that may be used ….to identify a specific individual).[134] According to common rules this phrase constitutes the element 'belonging to another' that is required as an element of identity theft. The Identity Theft Act 1998 and the Identity Theft Penalty Enhancement Act 2004 do not also determine whether the person that the means of identification belongs to is alive or dead or both. On this point, these statutes are considered ambiguous. Consequently, US courts have expansively interpreted identity theft laws and expanded their scope to encompass both living and dead persons.[135] It might be said that the US legislature should expressly state in the Identity Theft Act 1998 that the accused knows that the means of identification, which he transfers or uses belongs to another person whether that person is alive or dead.

Accordingly, if the Iraqi legislature wishes to adopt, or borrow the definition of another person's means of identification, it should expressly state that a person is guilty of identity theft if he intentionally obtains a means of identification that belongs to another person, irrespective of whether that person is alive or dead. It should also consider inclusion of the identities of legal persons that belong to legal persons, such as firms, corporations or any other entities.

---

[133] The element of possession has previously been criticised. It was stated that the possession cannot be an element of identity theft because when a person is requested to abandon it the *actus reus* and *mens rea* do coincide.

[134] 18 U.S.C. § 12028 (c) (C) (3) (3)

[135] *United States v. LaFaive*, 618 F.3d (7th Cir. 2010) at 616-17; *United States v. Maciel –Alcala* 612 F.3d (9th Cir. 2010) at 1101; U.S. v. *Zuniga-Arteaga*, 681 F.3d 1220 C.A 11 (Fla.) 2012

6.2.4 *Mens Rea* of Identity Theft

It can be inferred from the US provisions that are stated in either the Identity Theft Act of 1998 or the Identity Theft Penalty Enhancement Act of 2004 that the *mens rea* of identity theft consists of two elements: acting *knowingly* and *without lawful authority* transferring, using, and possessing a means of identification of another person.[136] The two elements of the *mens rea* of identity theft will be illustrated below.

6.2.4.1 Knowingly Transferring, Using or Possessing Another Person's Identity

To be guilty of identity theft the accused needs to know and be aware that he is transferring, possessing, or using a means of identification belonging to another person, without lawful authority, with intent to commit other crimes.[137] For instance, a person may be guilty of identity theft or aggravated identity theft if he knows that he is transferring, using, or possessing a means of identification of another person without lawful authority. In addition, he should know that this means of identification belongs to another person and is not false identity.

It does not appear from the formulation of the provisions that relate to *mens rea* of identity theft in either the Theft Act of 1998 or the Identity Theft Penalty Enhancement Act of 2004 that the accused must know that the means of identification belongs to another person. As a result, the courts in the US diverged into two groups. One group of judgments hold that the criminal must not know that he uses another person's means of identification without lawful basis and the State is not required to prove that the accused knows that he uses the means of identification without lawful basis.[138] Therefore, he is guilty of identity theft irrespective of whether he knows that he uses another person's means of identification or not. Whereas the second group of judgments hold that the accused should be aware that he is using another person's means of identification and the States should have to prove that the accused knew that he used another person's

[136] Identity Theft and Assumption Deterrence Act 1998, section 1028 (a) (7) Public Law No. 108-275, 108 Congress Ch. 47 title 18, § 1028 (a) (1)
[137] ibid; A Steel, supra, note 48, 519
[138] *Flores-Figueroa v. U.S.*, 556 U.S. 646, 129 S. Ct. 1886 (2009); *United States of America v. Gaspar*, 344 Fed Appx. 541(11th Cir. 2009); *U.S. v. Grajeda Gutierrez*, 372 Fed. Appx. 890 (10th Cir. 2010)

means of identification.[139] If the accused does not know that he uses another person's means of identification, he may not be guilty of identity theft. These two Acts have been criticised and labelled as ambiguous Acts.[140]

In the Identity Theft Penal Enhancement Act 2004, the *mens rea* of aggravated identity theft also requires that the accused should know that he is transferring, using, or possessing the means of identification during or in relation to any felony violation enumerated in subsection (c).[141] Consequently, if an individual is not aware that he is transferring, using or possessing a mean of identification of another person during or in relation to any felony violation enumerated in subsection (c) he may not be guilty of aggravated identity theft.

In addition, the issue of an intention to commit, aid, or abet another person to commit other crimes, which is required by the Identity Theft Act 1998 and the Identity Theft Penalty Enhancement Act 2004, may give rise to issues that should be taken into account by the Iraqi legislature. US courts, for instance, cannot apply the Identity Theft Act 1998 or the Identity Theft Penalty Enhancement Act 2004 if the accused intends to use another person's means of identification, but without intent to commit other crimes. On the other hand, it is uncertain whether these laws govern the case of possession of

---

[139] *United States v. Holmes*, 595 F.3d 1255 (11th Cir. 2010); *United States v. Ronald D. Adkins*, 372 Fed Appx. (6th Cir 2010); United *States v. Gomez-Castro*, 605 F.3d 1245 (11th Cir. May 13, 2010); *United States v. Gomez*, 580 F.3d 1229 (11th Cir. 2009); *U.S. v. Novas*, 461 Fed. Appx.896 (11th Cir. 2012)

[140] *United States v. Villanueva-Sotelo*, 515 F.3d 1234, 380 U.S. App. D.C. 11 2008; Similarly, the Court of Appeal in Kansas in the case of State of *Kansas v. Hardesty*, criticised the legislation of Kansas, which is similar to these Acts. The court stated that the legislator does not determine whether the word person comprises both live and dead persons. *Kansas v. Hardesty*, 42 Kan.App.2d 431, 213 P.3d 745 Kan. App., 2009

[141] Section (c) of the Identity Theft Penalty Enhancement Act 2004 states: definition.—For purposes of this section, the term 'felony violation enumerated in subsection (c)' means any offense that is a felony violation of—''(1) section 641 (relating to theft of public money, property, or rewards), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), or section 664 (relating to theft from employee benefit plans); ''(2) section 911 (relating to false personation of citizenship); ''(3) section 922(a)(6) (relating to false statements in connection with the acquisition of a firearm); ''(4) any provision contained in this chapter (relating to fraud and false statements), other than this section or section 1028(a)(7); ''(5) any provision contained in chapter 63 (relating to mail, bank, and wire fraud); ''(6) any provision contained in chapter 69 (relating to nationality and citizenship); ''(7) any provision contained in chapter 75 (relating to passports and visas); ''(8) section 523 of the Gramm-Leach-Bliley Act (15 U.S.C.6823) (relating to obtaining customer information by false pretenses "pretences"); ''(9) section 243 or 266 of the Immigration and Nationality Act (8 U.S.C. 1253 and 1306) (relating to wilfully "wilfully" failing to leave the United States after deportation and creating a counterfeit alien registration card); ''(10) any provision contained in chapter 8 of title II of the Immigration and Nationality Act (8 U.S.C. 1321 et seq.) (relating to various immigration offenses); or ''(11) section 208, 811, 1107(b), 1128B (a), or 1632 of the Social Security Act (42 U.S.C. 408, 1011, 1307(b), 1320a–7b (a), and 1383a) (relating to false statements relating to programs under the Act).''

another person's means of identification in which the criminal does not intend to use, but sells them instead.[142]

It could be said that if the Iraqi legislature intends to borrow or adopt this element of US *mens rea*, it should expressly state that the accused must know that the means of identification belongs to a legal or natural person (irrespective whether he is alive or dead); he must know that he uses a real identity and not a false identity (otherwise, he is not guilty of identity theft if he believes that he uses a false identity). The Iraqi legislature should consider the person who obtains, transfer, or uses another person's means of identification to be committing a crime irrespective of whether he intends to use it to commit other crimes, or not.

6.2.4.2 Borrowing or Adopting the Element of Without Lawful Authority

The term 'without lawful authority', which is stated in both the Identity Theft Act of 1998 and the Identity Theft Enhancement Act of 2004 gives rise to fundamental problems that may be faced by courts when they apply these laws to the accused because these two laws do not define or determine the term 'without lawful authority'. Therefore, the term 'without lawful authority' raises the issue of whether the means of identification of another person must be used, with or without, the person's permission to cause a violation of the Identity Theft Act of 1998 or the Identity Theft Penal Enhancement Act of 2004. If the accused uses the means of identification with the person's consent, does he violate US identity theft offence laws? In other words, does the term 'without lawful authority' equate to the term 'unauthorised,' if the person uses means of identification of another person with his permission? In such case, the accused does not violate the Identity Theft Act because he has permission from the owner of the identity to use that person's means of identification, and then the accused cannot be guilty of either identity theft or aggravated identity theft.

The term 'without lawful authority' has triggered a debate among US courts, particularly with respect to the application of the Identity Theft Penalty Enhancement Act 2004. US courts have held in many cases that the term 'lawful authority' does not equate to the term 'authorisation' and therefore these terms cannot apply

[142] M Gercke, supra, note 108

interchangeably.[143]

It can be argued that the term 'without lawful authority' should be given its ordinary meaning: it should refer to the transferring of, or the use of, another person's means of identification without the person's consent and be contrary to the law. However, if the means of identification is used with the person's consent, but contrary to the law, it is not identity theft. It may be violation of another law, but not identity theft. It might be said that the term without lawful authority is unsuitable to a condition or element of identity theft. If another person's means of identification has been obtained, transferred or used without his consent, identity theft is committed irrespective of whether the obtaining, transferring or the using of the means of identification is according or contrary to the law. The Iraqi legislature should not borrow or adopt this element when it intends to enact a new potential identity theft law.

To sum up this section, the aforementioned shortcomings that relate to the US *mens rea* element of identity theft, are considered fundamental shortcomings, consequently the Iraqi legislature should avoid repeating them when it intends to adopt or borrow the provisions that are set forth in US identity theft laws.

6.2.5 Punishments

The Identity Theft Act of 1998 provides a punishment, which can be applied to a person

[143] *United State of America v. Ozuna-Carbrera,* 663 F 3d 496 (1st Cir. 2011); In *U.S. v. Ozuna-Cabrera,* for instance, the United States Court of Appeal, First Circuit has held that "[R]egardless of how the means of identification is actually obtained, if its subsequent use breaks the law, specifically, during and in relation to commission of a crime ……it is a violation of § 1028 (a)(1) ." In addition, the court stated that "five other courts of Appeals have conclude that theft of the means of identification is not required to trigger criminal liability under § 1028(a) (1)", *United States of America v. Ozuna Carbrera*, ibid, 663 F d 500; *United Sates v. Lumbard*, 706 F.3d 716 C. A. 6 (Mich.) 2013. In other words, the accused will face criminal liability irrespective of whether the means of identification has been stolen or not and then used in fraudulent acts, or it is genuinely acquired. The court reasoned its decision that the Identity Theft and Assumption Act of 1998 was enacted to cover: [T]he commission, or aiding and abetting in the commission of 'any unlawful activity that constitutes a violation of federal law a felony under any applicable State or local law.' 'By contrast, the aggravated identity theft statute § 1028A (a) (1), covers 'any felony violation enumerated in subsection (c)':- a discrete list of federal felonies. The statutes are therefore distinguishable not by the method of procuring the means of identification, but by the underlying criminal conduct that they respectively target. Section 1028A (a) (1) is a logical extension of § 1028(a) (7), and punishes more severely those identity crimes committed during and in relation to a specifically enumerated subset of problematic felonies', *United States v. Retana*, 641F. 3d 272, 273-75 (8th Cir.2011); *United States v. Mobley*, 618 F.3d 539, 547-48 (6th Cir. 2010). In the same sense, the fourth Circuit held in the case *United States v. Abdelshafi* that another person's means of identification needs not necessary have been misappropriated. 592 F.3d 602 (4th Cir. 2010)

who knowingly transfers or uses one, or more than one, of a person's identifiers without lawful authority with the intent to commit any activity that constitutes a violation of federal law or which constitutes a felony under any applicable state or local law. This punishment will also be applied to the person who aids or abets in the commission of such activities. This punishment may sometimes be determined according to the values of the things that have been stolen during one year. For instance, if the items that have been stolen during one year are equivalent to $1,000 or more[144] the punishment is a fine and/or imprisonment for not more than 15 years. However, if the value of items that have been stolen is less than equivalent to $1,000,[145] the punishment may be a fine and/ or imprisonment for three years.[146]

It might be said that the above punishment is confirmation that the US legislature has failed to criminalise the act of *unlawfully obtaining* a person's means of identification. Therefore, when enacting the Identity Theft Act 1998, the US legislature intends to criminalise the transferring of, or using of, another person's means of identification rather than criminalising the act itself. The above describes a crime that has been committed by *using stolen* identity. Values of things that have been stolen during one year may be considered pre conditions to increasing or decreasing the punishment for crimes committed by using stolen identity, rather than increasing or decreasing the punishment of identity theft itself. The Iraqi legislature can adopt the above pre requisite condition of the punishment if it intends to criminalise the use of stolen identity as a stand-alone crime in itself.

6.2.6 Conditions That May Increase or Decrease the Punishment of Identity Theft

The Identity Theft Act of 1998 states certain conditions that may increase the punishment of identity theft, such as a previous conviction, facilitation of other crimes and violence during crimes.[147] These conditions are considered aggravating conditions, which may augment the punishment of identity thief. For example, if identity theft has been committed to facilitate other crimes, such as drug trafficking, or is associated with a crime of violence or has been committed by an offender with a former verdict against

[144] 18 U.S.C. § 1028 (b) (1) (d)
[145]18 U.S.C. § 1028 (2) (b)
[146] 18 U.S.C. § 1028 (2)
[147] 18 U.S.C. § 1028 (3) (a, b, c)

him, the punishment may be a fine and/or imprisonment for not more than 20 years.[148]

If the stolen means of identification has been used to facilitate an act of international terrorism the punishment will be a fine and/or imprisonment for 25 years.[149] Furthermore, the Identity Theft and Assumption Deterrence Act of 1998 has imposed confiscation as a penalty. The law stated that any device must be confiscated if it has been used, or intended to be used in the commission of identity theft.[150] The US legislature in the Identity Theft Penalty Enhancement Act 2004 increased the penalties of identity theft. It added two years imprisonment to the penalty if the criminal used the stolen identity to carry out other crimes. In addition, it added five years imprisonment for the punishment of the crime if the accused uses the stolen identity to commit terrorist crimes.[151]

It might be said that the above aggravating conditions are considered rational conditions that may assist in combating identity theft or deterring the unscrupulous persons from stealing people's means of identification, and then using it to commit other crimes. Accordingly, it is important that if the Iraqi legislature sets out these conditions in the new potential law to combat identity theft.

The author in his recommendations underpinned the view, which believes that the core element of the *actus reus* of identity theft is the illegal act of obtaining a person's means of identification. If some circumstances, such as the trust that may be given to people by their friends they are available they may make the commission of identity theft easy. Due to some identity thieves having been trusted by the victim, they can easily get his confidential information. In order to prevent unscrupulous persons from violating the trust that is afforded to them by the victim, the author observes that obtaining a person's means of identification by violation of the trust afforded should be an aggravating condition that increases the punishment for identity theft. Since, the US legislature does not criminalise the act of the unlawful obtaining of another person's means of identification; thus, it does not consider the violation of the trust that is afforded to the accused by the victim as an aggravating condition. The author suggests that it would be

[148] 18 U.S.C. § 1028 (b) (3)
[149] 18 U.S.C. § 1028 (b) (4)
[150] 18 U.S.C. § 1028 (b) (5)
[151] Identity Theft Penalty Enhancement Act 2004 Pub. L. No. 108-275, 1028A § 2, 118 Stat. 831

better if the Iraqi legislature considers some methods that are used to commit identity theft, such as theft inside the workplace, or theft between friends as aggravating conditions that may increase the punishment for identity theft. Methods like these make the commission of identity theft easy. The criminal who has a pre-existing relationship with the victim can access their information without any obstacle or hesitation.

6.2.7 The Discretion Given to the United States Sentencing Commission

Another issue, which is stated in the Identity Theft Act 1998, may cause a problem and violate the principle of legality if it has been adopted without modification by the Iraqi legislature, namely the issue is the discretion that has been given to the United States Sentencing Commission to make identity theft an aggravated crime if it associated with certain conditions. The US legislature has directed the United States Sentencing Commission to make identity theft as an aggravated crime when it is associated with certain instances, such as using device making equipment to commit identity theft; or where there was an unauthorised transfer or illegal utilisation of any methods of identification to create or obtain other means of identification; or where the perpetrator owns five or more means of identification, which were illegally produced from another means or obtained by using another person's means of identification.[152] The Identity Theft Act entitles the Sentencing Commission a power to raise the level of the identity theft offence to level 2 or 4 if it has been committed by multiple criminals.[153]

It could be argued that the above discretion that is given to the United States Sentencing Commission may be considered a legislative function according to the Iraqi legal system. Judges or law enforcement officials cannot exercise this function. If they do, they may violate the principle of legality that confines the legislative function to the legislature only. Consequently, the Iraqi legislature should ensure that any such aggravating circumstances are set out in the potential new identity theft Act rather than allow judges or law enforcements officials to impose them.

6.3 Recommendations

The previous analysis in this chapter regarding both UK laws and US identity theft laws

[152] United States Sentencing Guidelines § 2b1.1 (11) 2011
[153] U.S.S.G. § 1B 1.3 (2011)

showed that there are two approaches, which may be used to govern and combat identity theft: the United Kingdom's approach and the United States' approach. In the US's approach, legislation is considered the sole source of criminal statutes, while the UK's approach depends on both legislation and precedent cases (the common law). Therefore, there are two resources for criminal statutes in UK: legislation and case laws. With respect to the UK's approach, it is impossible for this legal framework to be adopted absolutely in the Iraq legislation, because there are huge differences between the two systems. There is no rapprochement between them because the Iraqi system depends on a civil law system in which the legislation is considered the sole source of criminal law.

In addition, Iraqi legislation espouses the principle of legality, which prevents judges from extending the current theft offence laws or from creating new ones. The principle of legality may be an obstacle that prevents the application of the UK's approach to Iraqi legislation. The principle of legality and its corollaries of clarity and precision require legislative criminal legal provisions that criminalise an illegal activity, such as identity theft, to be complete and specific, while the provisions in the UK law that governs identity theft is broad-based legal provisions, which does not govern identity theft with required defence of specificity.

However, as was shown in the section one of this chapter, there are many provisions stated in both the Fraud Act 2006 and the Computer Misuse Act 1990, which can be adopted or borrowed by the Iraqi legislature to criminalise some sophisticated methods (such as phishing, spam, unauthorised access, or hacking as stand-alone as crimes).

Section two of this chapter contained the analysis of the US's approach. The first thing that may be borne in mind that there is similarity between both the US and Iraqi legislation because both US and Iraq contain the principle of legality in their legislation, which confines the ability to delineate a crime and set out a punishment to the legislatures and prevents judges from doing so. In both regimes, judges cannot create crimes and set out punishments, therefore, there is no obstacle facing the Iraqi legislature if it seeks to adopt or borrow provisions from US legislation. As a result and despite the flaws that were explored and determined in US identity theft laws, it could be said that provisions that were stated in these laws may be the best provisions to look

for inspiration which can be adopted or borrowed by the Iraqi legislature to enact a new comprehensive law to govern identity theft.

However, adopting or borrowing provisions from US identity theft laws raises the following question: what steps that should the Iraqi legislature take to criminalise the act of the illegal obtaining of another person's means of identification without their consent, and then using it to commit other crimes. The Iraqi legislature should take some steps to criminalise obtaining another person's means of identification without their consent, and then using it to commit other crimes. The next section will illustrate these steps.

6.3.1 Elements to Be Taken to Criminalise Identity Theft in Iraq

There are many elements that the Iraqi legislature should consider and determine when it comes to setting out provisions to govern the appropriating of another person's means of identification without their consent, and then using it to commit other crimes. These elements are as follows: definition of the unlawful act that is considered as *actus reus* of identity theft, and determining the elements of this act. The Iraqi legislature should set out provisions in the potential identity theft Act to deal with circumstances that constitute participation in identity theft, particularly to deal with the case when one person has stolen information, but it then used by somebody else to commit other crimes. In other words, occasionally, the person who uses another person's means of identification or personal information to commit other crimes may not be the same person who stole it

In addition, the legislature should determine the elements of the state of mind of the person who obtains another person's means of identification, and then uses it to commit other crimes. These parameters will be addressed below.

6.3.1.1 Definition of Identity Theft

As shown previously, there is no universal agreement whether identity theft is a crime in itself. Consequently, there is no universal definition of identity theft.[154] In addition, there is no agreement about the definition of identity theft, or what precisely it is, even

[154] Section one of second chapter of this thesis, 8

within the scope of legislation of the States that have considered it as a crime.[155] Scholars also espouse multiple trends with respect to the definition of identity theft.[156]

From a legal point of view, the definition should be an 'omnibus' definition and refer to all elements of identity theft. Otherwise, it may be ambiguous. The ambiguous definition of identity theft offence may cause problems when the courts attempt to examine and determine the elements of it. If the Iraqi legislature does not define it adequately, in specific law, it will not be easy to prepare a charge against identity theft criminals. Although the definition that is stated in the Theft and Assumption Deterrence Act 1998 is broad and contains some aspects of fraud, it may be an acceptable definition.[157]

If the Iraqi legislature adopts the definition that is stated in the US Identity Theft Act 1998, it should avoid the shortcomings[158] that were determined in the previous section. The Iraqi legislature should redefine identity theft clearly to ensure that there is no ambiguity in it that may be triggered when the courts apply the potential new Act to identity theft cases, otherwise the principle of legality may be violated. The principle of legality requires the definition of any act to be omnibus and refer to the distinctive features of the illegal phenomenon, which is represented here in identity theft.

In second chapter, a definition for identity theft was suggested. Identity theft should be defined as knowingly and willingly or recklessly and dishonestly obtaining by any method whether sophisticated or not, personal or financial information of another person whether legal or natural person, transferring of or using it without that person's consent, and then possibly using it to commit or aid or abet in the commission of other crimes.

[155] Section one of second chapter of this thesis
[156] ibid
[157] This Act defines identity theft in section 1028(a)(7) as when an individual knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law"
[158] Although the definition is broad, the US legislature does not criminalise the act of the illegal obtaining of a person's means of identification. It considers the possession of the person's means of identification as an element of identity theft. The possession cannot be an element of identity theft. Finally, it does not consider the illegal transfer or use of a company, corporation's means of identification, or any other entity as a crime.

6.3.1.2 Ingredients of Identity Theft

According to academics' literature and legislation in other jurisdictions, identity theft consists of two main ingredients: *actus reus* and *mens rea* and a third element a means of identification is referred to as the subject of crime. According to the clarity and precision of criminal law that it is required by the principle of legality, an identity theft offence should precisely be defined. Its ingredients should also be determined in advance. Consequently, the Iraqi legislature needs to determine these elements accurately.

As stated in the previous section, the US legislature afforded an array of choices that the Iraqi legislature can borrow from. However, the main flaw of these choices is that the US legislature does not criminalise the act of the unlawful obtaining of another person's means of identification. As a result, in the next sections, the author presents potential ingredients of identity theft that may assist the Iraqi legislature to enact a comprehensive law to govern identity theft.

6.3.1.2.1 *Actus Reus*[159]

The a*ctus reus* of identity theft means an act that may be committed by the perpetrator(s) to obtain another individual's means of identification. It also can include the transferring, selling, offering for sale or using another person's means of identification to commit other crimes. The author in his recommendations differs from the US legislature that considers the transferring and using the means of identification of another person the principal ingredients of identity theft.

The author suggests that the main ingredients of identity theft are the act of the unlawful obtaining of another person's means of identification, transferring, selling, offering for sale or the use of it for the criminal own purpose. Therefore, the author recommends that the Iraqi legislature should take into account these ingredients when it intends to enact a potential new Act to cover identity theft.

The wording of the potential *actus reus* as an element of identity theft will be as: a person is guilty of identity theft if:

[159] Section one of chapter three

1. He knowingly and willingly or recklessly and dishonestly, without consent *obtains* the personal or financial information of another person for their purposes.

2. Or after legally or illegally obtaining another person's means of identification, he knowingly and willingly or recklessly *uses* another person's means of identification or their financial information to commit other crimes, or aids or abets in the commission of these crimes.

3. If he Transfers, sells, offers for sale, distributes, or makes the use of personal or financial information of another person available for others knowing that (or being reckless as to whether such information would be or might be, used to commit a punishable crime.

6.3.1.2.1.1 Criminalising Some Sophisticated Methods

Sophisticated methods as a means to commit identity theft are other issues that may give rise to problems and need specific attention from the Iraqi legislature. The advent of the internet has changed methods that can be used to commit such crimes. Most crimes, such as identity theft offences, were committed by using traditional methods. However, with advent of the internet, new processes to commit crimes have emerged and the perpetrator(s) have discovered new methods to commit identity theft crimes. As stated in chapter three, criminals can use sophisticated methods (such as phishing, spyware, hacking, or Trojan Horse).[160]

The US legislature in both the Identity Theft Act 1998 and the Identity Theft Penalty Enhancement Act 2004 does not criminalise some methods that may stand alone as crimes.[161] Consequently, the author recommends that the Iraqi legislature should put a new Act in place to criminalise sophisticated methods of internet crimes, such as phishing, hacking, and spyware.

Two types of legislation can be used to criminalise an illegal act: a specific-act approach and a multiple-act approach. The specific-act means that the legislature enacts a new Act to govern the new illegal act, which was not crime under the previous Act.

[160] ibid Section one of chapter three
[161] See section two of chapter three of this thesis

This specific-act contains provisions govern only the illegal act. They do not govern the subsequent crimes or the means that is used to commit the new crime if this means stands as a stand-alone offence. The legislature would need to enact another Act to govern the subsequent crimes or the means that is used to commit the new illegal act if those crimes are not governed by other laws. In contrast, a multiple-act approach means that the legislature should enact one piece of legislation that contains numerous or comprehensive provisions to govern both the new illegal act, the methods that are used to commit it or the subsequent crimes.[162]

With respect to identity theft, as was shown in chapter three, some methods that are used to commit identity theft stand as stand-alone crimes.[163] The author suggests that the Iraqi legislature should adopt the multiple-act approach that governs both identity theft and the methods that are used to commit it.

6.3.1.2.1.2 Participation in Identity Theft

Participation in identity theft is not an element of the elements of identity theft. However, it is according to Arabian scholars' opinions[164] considered a subset of the *actus reus* of identity theft. Participation in identity theft means two or more perpetrators are jointly involved in the commission of an identity theft offence.[165] Participation can be divided into two types: principal participation and secondary participation.[166] The definition of participation and the types of it have been discussed in chapter three of this thesis. Putting specific provisions in place that govern participation in identity theft in the possible potential identity theft offence law has become an urgent issue because participation may facilitate identity theft commission; particularly identity theft needs more than one person to be committed. Especially, after the internet has become the main source of personal information for perpetrators, identity theft is now often remotely committed. Many organised gangs are involved in

[162] Warren B. Chik, supra, note 83, 24

[163] Phishing is one of many that are used to obtain people's means of identification. Hacker also is a means that is used to commit identity theft and it stands as a crime in itself.

[164] M R Bara, *General Principles of Libyan Penal Code*, (Khatraa Company 2010 K), 348; A F Soruor, Al- Waseet in Criminal Law, (6th edn, Dar Arabic Nahda, Cairo 1996) 398

[165] M M Mustapha, *Penal Code Explaining* (Cairo 1974) 324

[166] See section two of chapter three of this thesis: The principal participation means the accused may commit one or more than one of the elements of identity theft, such as gathering another person's means of identification, whereas secondary participation means a person or persons may aid, abet, consult, and incite another person to commit identity theft.

identity theft. Most members of gangs locate in different places or different countries, therefore, it is difficult to detect and catch perpetrators of identity theft.

According to the term 'participation', some criminals may not commit the substantive ingredients of identity theft, thus they may not be subject to the punishment that the law sets out for criminals who commit substantive identity theft.[167] Consequently, the Iraqi legislature should set out rules beside the rules that govern the principal perpetrators to govern principal and secondary participants who are involved in identity theft. The author proposes this suggestion of the potential legal text of participation in identity theft: a person is guilty of participation in identity theft if he knowingly and willingly plans, commits identity theft, instigates, encourages, agrees with, orders another individual to commit identity theft, or aids or abets in commission of identity theft.

The author recommends that Iraq should hold a convention with other countries to regulate extradition of identity thieves. In addition, as stated in chapter one, identity theft has become a threat to most world States' economics. Therefore, it could be said that identity theft should be considered a universal crime, and that every State, which apprehends the perpetrator of identity theft on its territory should prosecute him or her according to its criminal law. To make this proposal effective and adequate, the Iraqi legislature should provide a section in the potential Act of identity theft in which the legislator considers identity theft, which is committed beyond Iraqi's borders a crime just as if it was committed on Iraqi's soil.

6.3.1.2.1.3 Inchoate Identity Theft[168]

Inchoate identity theft means the criminal shows intent to commit identity theft, but somehow does not complete all its elements. The author recommends that the Iraqi legislature should consider the act of the merely obtaining another person's personal information without consent, with intent to commit other crimes, as an offence *irrespective of whether it is used* to commit other crimes, such as fraud, or not. Additionally, it should consider an inchoate identity theft to be a complete identity theft. In other words, it should equate inchoate identity theft and substantive identity

[167] The substantive identity theft means a crime that does not have as an element the performance of some other crime.
[168] for more information about inchoate of identity theft see section two of chapter three of this thesis 4

theft in terms of punishment.

6.3.1.2.2 Means of Identification

The means of identification or what is so-called 'property' is also an element of identity theft that is recommended to the Iraqi legislature to set out in the potential identity theft Act. It was shown in chapter four when the existing theft offence laws in Iraq were analysed, that there was disagreement between judges and scholars about whether personal information can be considered as property.[169]

In his recommendation regarding the above issue, the author suggested that the Iraqi legislature should consider a person's means of identification as a specific type of property in order to protect it from the unlawful use by unscrupulous persons to commit other crimes. It could be said that personal information as a means of identification can be considered a *fictional property*. The principle of legality would oblige the Iraqi legislature to define the means of a person's identification as subject to theft precisely. As was stated in previous section, the definition of means of identification that is found in the Theft Act 1998 is a workable definition. The author recommends that the Iraqi legislature should adopt either it or the following modified definition: a means of identification means any information whether biological or physiological, such as a finger print, voice print, retina or iris image, deoxyribonucleic acid DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit and debit cards numbers, social security number, financial institution account number, passport number, password and driver licence number that is usually used, alone or in combination with other information, to identify or aims to identify a person.[170]

It is worth stating that not every means of identification should be protected by the new potential identity theft Act; only the means of identification that belongs to another person may be subject to legal criminal protection.[171] The author recommends that the Iraqi legislature should state in the potential identity theft law, that the means of

[169] Section two of chapter four of this thesis
[170] Section 402.1 of Criminal Code of Canada 2009 c 28 s 10 (R. S. C., 1985, c. C. 46)
[171] For example, some means of identification, such as an old person's password, his old credit card number or his old address is considered an abandoned means of identification, thus it cannot be subject to theft unless it is used with his current means of identification.

identification (as a subject of identity theft) should be means of identification belongs to the person who has a right to use it to define himself.

6.3.1.2.3 *Mens Rea* of Identity Theft

Due the nature of a person's means of identification the theft of it does not cause permanent deprivation of the person of it. There is disagreement between judges as well as academics with respect to this issue.[172] The author suggests that the theft of a person's identity is taking place irrespective of whether the obtaining of these identities is permanent or temporary. As a result, in this study, the Iraqi legislature is recommended to insert, in specific legislation, that when a person obtains another person's means of identification without their consent, then that person commits a crime irrespective of whether the obtaining of this means is permanent or temporary. In conclusion, the author can summarise the elements of identity theft as: a person is guilty of identity theft if.

(1) He knowingly and willingly or recklessly and dishonestly, without consent *obtains* the personal or their financial information.

(2) Or after legally or illegally obtaining another person's means of identification, he knowingly and willingly or recklessly *uses* another person's means of identification or their financial information to commit other crimes, or aids or abets in the commission of these crimes.

(3) If he transfers, sells, offers for sale, distributes or makes the use of personal or financial information of another person available for others knowing that (or being reckless as to whether) such information would be or might be, used to commit a punishable crime.

6.3.2 Punishment for the Crime of Identity Theft

It might possible to be said that the punishment of a simple identity theft crime should be 5 years. However, some identity thieves are more dangerous than others, and some of them have a previous criminal record. Other thieves may exploit the trust afforded to them by their friends, employers, companies, financial institutions, or government

[172] Section two of chapter four of this thesis

institutions. In addition, many perpetrators may be involved in a conspiracy to commit identity theft. The aforementioned cases may be considered aggravating conditions that justify the increasing of the punishment of identity theft. It is possible to say that the punishment of identity theft associated with aggravating conditions is 15 years. If the stolen identity has been used to commit crimes against person's financial status, such as open a new account in the person's name, or perpetuating his account the punishment should be 20 years. The author recommends that the Iraqi legislature should take these conditions into account when it drafts the potential identity theft law. Reasons behind this harsh suggested punishment are; identity theft is a crime that is committed primarily to facilitate other crimes. It is easily committed. It ruins the economy of the State. Sometimes it is committed remotely, thus it is difficult to detect and adherent the identity thieves to prosecute them because they do not leave any trace, which may lead to them and their arrest. The main reason to suggest a harsh punishment for identity theft is some criminals are not deterred by a light punishment.

Someone might argue that even the harsh sentence will not solve the problem: in other words, even if the Iraqi legislature adopts or borrows provisions from either the UK or the US legislation, or it takes into account the above recommendations to enact a comprehensive law to govern identity theft. It may still be ineffective and inadequate to prevent the commission of identity theft completely. The question is how effective measures can be taken to prevent identity theft, since some criminals have not been completely deterred by punishment. The criminal may be deterred by the penalties,[173] if he thinks logically,[174] but increasing the penalties may be a deterrent for criminals, who are arrested, but not for those who are not caught, or who do not leave any evidence that may lead law enforcement officials to apprehend them. For instance, they may use sophisticated methods, such as 'anonymiser' software to commit identity theft and hide any trace.[175] Moreover, many identity thefts are committed via the internet remotely,

[173] D McCullagh, 'Season Over 'Phishing'?' CNET News com July 15 (2000) available at <http://zdnet.com/2100-1105_2-5270077.htm1> accessed on 2 February 2011

[174] Gary M Victor, 'Identity Theft, Its Environment and Proposal for Change' (2006) Vol. 18 (3) Loyola Consumer Law Review 273-309

[175] James K Robinson, 'Remarks at the International Computer Crime Conference: Internet as the Scene of Crime' (2000) available at <http://www.usdoi.gov/criminal/cybercrime/roboslo.htm> viewed on 8 April 2012

and the criminals do not foresee that they may be arrested.[176]

In addition, as Victor[177] observes, increasing penalties may reduce ordinary individuals' vigilance, making them less likely to protect their personal information. In effect, although the role of the law is very important in fighting identity theft and reducing individuals' risk, the law alone cannot prevent identity theft. Therefore, all the identity theft parties should work together to stop this plague on society.

6.4 Conclusion

This chapter has examined whether, and to what extent, the Iraqi legislature should adopt or borrow a legislative solution from either both the UK and US legislation to counter the inadequacy that is found in Iraq's theft offence laws, the Information Crimes Project 2011 and existing judicial solutions to combat identity theft.

In section one, UK laws, including the Data Protection Act 1998, Theft Act 1968, Fraud Act 2006 and Computer Misuse Act 1990, which all may be used to counter various elements of identity theft were analysed. The study showed that the Data Protection Act of 1998 dealt with principles that can be used to regulate data registration and how data controllers comply with this Act. It is also showed that the Act contains civil and administrative remedies, rather than criminal penalties. Therefore, the author believes that the provisions of that Act are inadequate to prevent identity theft, and would advise the Iraqi legislature not to adopt or borrow provisions from it to combat identity theft in Iraq.

The study also analysed the UK Theft Act 1968 and showed through this analysis that this Act suffers the same lacuna that existing theft offence laws in Iraq suffer from.[178] Consequently, the Iraqi legislature should not adopt or borrow provisions from it to combat identity theft. In order to complete the investigation, a number of cases were analysed to investigate how UK courts have dealt with the act of the unlawful obtaining

[176] D McCullagh, supra, note 173
[177] Gary M Victor, supra, note 174, 297
[178] The provisions of the Theft Act 1968 have been enacted to deal with tangible properties. They cannot cover the illegal obtaining of the intangible properties, such as people's means of identification. They cannot cover these properties because they cannot be subject to be physically taking. The provisions of the Theft Act 1968 requires permanent deprivation of the owner of his property associated with the illegal taken of the person's property to be theft, whereas there is no permanent deprivation to the person when his means of identification has been taken.

of another person's means of identification. It was shown that courts focused their effort on the fraudulent activities that were used to obtain other person's property, rather than the identity theft itself.

The provisions of the UK Fraud Act 2006 were also analysed. It has appeared from the analysis of those provisions that the UK legislature has created a general fraud offence.[179] The study showed that the UK legislature concentrated on the unlawful act, rather than the result of the act. The author has concluded that the concentration of the Fraud Act on the unlawful act, rather than the result of the act may be considered as a tool to combat some sophisticated methods, such as phishing and other malicious programs, which can be used to acquire personal information. In this case, the author recommends that the Iraqi legislature could adopt or borrow some of that Act's provisions to amend Iraq's fraud offence laws, particularly those laws were enacted dealing with conventional fraud offences, as well as to fight some sophisticated methods that are used to commit identity theft (such as phishing or pharm).

The analysis of the UK laws also extended to encompass the provisions of the Computer Misuse Act 1990. This analysis demonstrated that provisions of the Computer Misuse Act 1990 have been enacted to protect the integrity of computers, rather than the information that they hold. As a result, it was shown that these provisions are ineffective and inadequate to combat and prevent identity theft, particularly, when authorised access can be used for illegal purposes. However, the UK courts sometimes rely upon this Act to judge a person who gains unauthorised access to any computer and steals another person's means of identification. Irrespective of flaws that this law has, which may make it inadequate to cover identity theft, it might be helpful and the author recommended that the Iraqi legislature could adopt or borrow some its provisions to protect the integrity of computers that are connected to internet, particularly as Iraq has no specific provisions currently to deal with the misuse of computers and the internet.

In section two of this chapter, the study examined the possibility of adopting or borrowing provisions from US legislation that relate to identity theft: the Identity Theft

[179] This offence can be committed in three ways, specifically through making a false representation, failing to disclose information and abusing the position of trust with the intention of obtaining gain for the offender or for another person or to cause loss to another or expose another person to a risk of loss.

and Assumption Deterrence Act 1998 and the Identity Theft Penalty Enhancement Act 2004. The Identity Theft and Assumption Deterrence Act 1998 considers identity theft as a Federal crime.

The study showed that these two laws contain some drawbacks when they have come to deal with identity theft. On the one hand, the Identity Theft and Assumption Deterrence Act 1998 is described as too broad because it criminalises some illegal activities and considers them as identity theft offences, although they may fall within the scope of fraud offences. The accused who transfers or uses another person's means of identification to commit fraudulent activities, such as bank fraud, credit fraud or mail fraud may be subject to the Identity Theft Act, the Mail Fraud and Other Fraud Offences Act[180] and the Fraud Act.[181]

Officials in the Justice Department Criminal Division mentioned that federal prosecutors endorsed the broadening of the Identity Theft Act. They stated that this broadening in the definition of identity theft is needed because identity theft is rarely a stand-alone crime.[182] The federal prosecutors' views indirectly refer to the flaw in the Identity Theft Act, which was determined by the author, identity theft should be a stand-alone crime, and the US legislature should criminalise the act of the illegal obtaining of a person's means of identification. The US legislature criminalises the transfer of, or use of the means of identification of another person *rather than* the act of the unlawful obtaining of this means. In present circumstances, law enforcement officials are unable to use this law to prevent identity theft or to reduce its risk. Consequently, the US legislature enacted the Identity Theft Penalty Enhancement Act 2004 to boost the Identity Theft and Assumption Deterrence Act 1998 and to prevent identity theft.

The study showed that the Act (as the former 1998 Act) does not criminalise the act of the unlawful obtaining of another person's means of identification: this perpetuates a major flaw in the US approach. The study also demonstrated that both the Identity Theft and Assumption Deterrence Act 1998 and the Identity Theft Penalty Enhancement Act

[180] Mail Fraud and Other Fraud Offences 18 U.S. Code Ch.63 Pub. L. 113-65
[181] Mail Fraud and Other Fraud Offences 18 U.S. Code Ch.63 Pub. L. 113-65; Fraud and Swindle §1341
[182] United States General Accounting Office, GAO, Report to the Honorable Sam Johnson House of Representatives, Identity Theft Greater Awareness and Use of Existing Data Are Needed, 2002 available at <http://www.gao.gov/new.items/d02766.pdf> accessed on 17 Jan. 2014

2004 do not determine whether the person that the means of identification belongs to, is alive or dead: this leads to uncertainty as to the legislation's scope. In addition, it showed that the term 'without authority,' which is stated in these laws is ambiguous. Therefore, courts construed it to encompass the use of the means of identification with the owner's consent, contrary to law.

Notwithstanding these lacunae, the author recommended that the Iraqi legislature could adopt or borrow provisions from US identity theft laws to combat identity theft and fill in the gap that appeared in the current Iraqi theft offence laws and Information Crimes Project 2011. In order to appreciate whether the Iraqi legislature should adopt or borrow provisions from the UK or the US legislation, the study showed that the US's approach, although identity theft laws of the US have drawbacks might be the best approach that can inspire Iraqi legislation. Therefore, in order to enact a new law to govern identity theft, the author has recommended that the Iraqi legislature should adopt or borrow certain provisions from US identity theft laws, but only after avoiding the shortcomings that appear in them.[183]

Finally, the author has attempted to draw certain recommendations and circumstances that the Iraqi legislature should take them into account when it intends to create a new Act to deal with identity theft. Some of these recommendations might be helpful for the Iraqi legislature when it intends to enact a comprehensive law to govern identity theft. The author recommends that the Iraqi legislature needs to define identity theft and determine its elements precisely so that the principle of legality is respected. In addition, it should set out an appropriate punishment that may be applied to a person who commits this crime.

The study in its recommendations showed that legislatures in different jurisdictions use different approaches to criminalise the illegal activities, a specific-act approach, or a multiple-act approach: the author recommends that the Iraqi legislature should adopt the multiple-act approach to criminalise identity theft and some sophisticated methods that are used to commit it.

[183] The US legislature does not criminalise the act of the illegal obtaining of a person's means of identification. It considers the possession of the person's means of identification as an element of identity theft. The possession cannot be an element of identity theft. Finally, it does not consider the illegal transfer or use of a company's means of identification as a crime.

Chapter Seven

Conclusion and Recommendations

Introduction

Evidence from the current study demonstrated how that Iraq has no specific law that explicitly deals with identity theft as a crime. This implies that there are no provisions to deal with identity theft in Iraq, thus raising concerns as to what constitutes identity theft as well as determining its elements. Thus, the author proposes a legal framework that the Iraqi judges could use to deal with identity theft. In the preceding chapters (Chapter Three/Four), the contemporary theft offence laws in Iraq were analysed in order to assess whether these laws could adequately provide an effective legal framework to addressing identity theft. The analyses reveal that those laws would still not be sufficient to address a certain key of identity theft crimes.[1] The author went further in chapter five to examine whether judges in Iraq could extend existing theft offence laws to govern identity theft. Additionally, US and UK identity theft legislation was assessed and the review showed that while Iraq could alternatively adopt those legal frameworks in addressing identity theft crimes. That approach would present challenges associated with adopting UK and US identity theft legislation.

This final chapter has three parts: first part summarises the difficulties faced by the Iraqi judges in governing identity theft with current theft offence laws. How the Iraqi judges could adopt UK and US legal frameworks on identity theft will be discussed in the subsequent part. Finally, recommendations for effective implementation of the identity theft legislation in Iraq will be prescribed. The concluding part outlines suggestions for further study.

7.1.1 Background and Analysing the Nature of Identity Theft as a Crime

The review in current study revealed that identity theft crimes in Iraq were not defined. Extrapolating from existing general literature including courts' decision of several jurisdictions, the thesis found no significant indication that the act of the unlawful

[1] Existing Iraqi theft offence laws are inadequate to govern identity theft because they deal with the appropriation of tangible, while another person's means of identification is intangible thing. Tanking a person's identity theft causes challenges to Iraqi courts: the means of identification cannot be a subject of theft, it cannot be subject to physical taking and finally there is no permanent deprivation for the person of his identity when it being by the criminal.

access to a person's information constitutes identity theft. Most literature including judges' rulings seem to label or consider the use of another person's means of identification without his consent, with intent to commit other crimes, as identity theft. In effect, *the use* of another person's means of identification rather refers to the use of 'stolen identity to commit other crimes,' instead of theft of identity *per se*. The use of stolen identity to commit other crimes is a consequence of identity theft, but at sometimes, it is also a preparatory act to the commission of other crimes. This study illustrates that other crimes, which are committed by *using* a stolen means of identification may not be classified as identity theft. The categorisation of the use of another person's means of identification to commit other crimes as being identity theft, can only occur when the accused obtains another person's means of identification rather than when the suspect uses the means of identification to commit other crimes.

This thesis had demonstrated that Iraq has no specific law to address identity theft.[2] Review in Chapter 2 illustrated that existing Iraqi theft offence laws are used to deal with identity theft. The review indicated that Iraq has no coherent definition of identity theft, as the current theft offence laws are in use to deal with only physical property. In addition, even the Iraqi Penal Code 1969 review (otherwise called the Information Crimes Project established in 2011) did not clearly define identity theft.

In theory, the principle of legality requires that in order to criminalise an illegal act, such an act must be clearly defined. Drawing from existing general literature including professional views on identity theft and its elements, the current study proposes legislative measures Iraq could take to curb identity theft crimes. Chapter 2 various definitions of identity theft were considered. Definitions used by the US, states of Australian, and Canadian legislations the UK Home Office.[3] However, of those definitions reviewed, this study found that there is no universal definition of identity theft.

---

[2] See Chapter 1of this thesis

[3] S7 (1) Identity Theft and Assumption Deterrence Act of 1998**,** Pub. L. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998), *codified at* 18 U.S.C. §1028; South Australia Criminal Law Consolidate Act of 1935 s 144C amended in 2003; Queensland Criminal Act of 1899 s 408D ins 2007 No. 14 s16 and amended in 2010 s 1 (4);Bill s 4 Act amended Identity Theft and Related Misconduct 404, 2(1) Canada 2009 available at <http://www.cba.ca/contents/files/submissions/sub_20090603_01_en.pdf> accessed on 25 May 2011; Home Office, 'Identity Crime Definitions' 2006 available at <http://www.identity-theft.org.uk/definition.html> accessed on 26 May 2011

The absence of a globally argued definition of identity theft does not mean that none of those definitions could fit or be applied in Iraq. One definition of identity theft proposed by the US Identity Theft and Assumption Deterrence Act 1998 seems to be appropriate for Iraq. Even though the US identity theft crime law does not clearly define the act and it provides no clear indication for measuring the act. However, above all, the law spells out punishment to actors. It could be guidance for the Iraqi legislature, thus the Iraqi legislature could adopt it.

The features of identity theft and factors that may contribute in the commission of identity theft were examined in Chapter 2. The review indicated that identity theft has unique features, which makes it different from identity crime and identity fraud. There are many factors involved in identity theft that precipitate and aggravate the act. The use of the internet is one of these factors: that why some legal professionals relate identity theft to internet crime. However, this study showed that associating identity theft crime with internet crime could be misleading, as the internet may be only a tool used to commit identity theft.

The current study highlighted the risks and impacts of identity theft. Evidence from the present study revealed that no single person is immune from identity theft. The victims of this crime in society can be children, adults, old, and deceased persons. With regard to the types of identity theft that were examined, the review indicates that identity thieves devise many ways of committing the act, as some of culprits are opportunistic criminals.

Chapter 3 analysed elements of identity theft based on the existing general literature. The review showed that in most legislation that deal with identity theft as a crime, legislatures logically only criminalise the use of, or the transferring of, another person's means of identification.[4] Nevertheless, the legislation does not seem to criminalise the unlawful act of obtaining a person's means of identification.

The review also showed that there are two types of methods used to commit identity theft: sophisticated and non-sophisticated methods. It was revealed that the identity theft consists of two main elements: the *actus reus* and *mens rea* and a third element a

[4] Identity Theft and Assumption Deterrence Act 1998 § 1028 (a) (7) Public Law 105-318, 112 Stat. US; South Australia Criminal Law Consolidate Act of 1935 s 144C amended in 2003

means of identification is referred to as the subject matter of crime. With respect to the *actus reus*, it was argued that this element is specific in nature, as identity thieves often use two types of methods to commit their crime: traditional or non-sophisticated methods, such as mail stealing or scouring trash and non-traditional or sophisticated methods, such as phishing or hacking. Some of these methods are not illegal *acts per se* while others are illegal, and regarded as crimes. Often, most of these methods of committing the act took place in non-physical actions.

Nowadays, phishing and other malicious programs used to commit identity theft and other computer related crimes, stand alone as crimes. Of the two forms of methods, this review demonstrated that cases of identity theft committed by traditional methods, seem to be more common than cases of identity theft that are committed by non-traditional methods. In addition, the study showed that there are several groups of individuals often involved in the commission of identity theft. In some cases, identity theft involves international organised crime; with some of the members of the identity theft crime groups being located in different continents, regions or countries. The thesis takes the view that the identity theft offence is a global crime, thus addressing it should involve a globally agreed effort or legislation. In the next section the challenges associated with curbing identity theft using theft offence laws in Iraq will be considered.

7.2 Actions recommended to Be Taken Either by Iraqi Judges or the Legislature to Overcome the Lack of Provisions Dealing with Identity Theft.

One of the key thrusts of the current study was to assess the efficacy of Iraqi legislation on identity theft crime, in particular whether existing Iraq theft offence laws are applicable to offences of identity theft. In other words, the research assessed whether the elements of the identity theft offence satisfy the elements of the offence of theft. Elements of offence of theft in this context are the *actus reus*, which is represented by the term ‘appropriation’, a person’s property as subject to theft, as well as depriving owner’s property ‘*mens rea*’. The above question then raised other questions, such as can personal information property be taken or carried away like movable property?; is a person’s means of identification property?; could the owner of a personal information be deprived of property in this information if is taken away? To answer these questions, the author analysed the Iraqi theft offence laws and also US and UK theft offence laws

were analysed.

A question might be raised when the answers to the above questions are "no" is whether the Iraqi criminal judge can extend the current theft laws (or create a new offence) to govern identity theft and determine a punishment for it. The role of the judge in extending the current theft offence laws (or creating new laws) gives rise to the issue of whether the role of judge to extend theft offence laws is considered to be a violation of the principle of legality.

Finally, if theft offence laws are inadequate to govern identity theft and the criminal judge cannot overcome this inadequacy by extending the scope of existing theft offence laws (or creating a new offence), how would the Iraqi legislature address this form of crime.

7.2.1 Difficulties That May Be Posed by the Application of the Current Iraqi Theft Offence Laws in Dealing with Identity Theft

From viewpoint of criminal law, the thesis assessed whether unlawful acts pertaining to identity theft could fall within the scope of existing law. The study showed that there are no specific provisions that can effectively govern identity theft. Due to identity theft being a crime that is committed to facilitate other crimes, such as fraud, the study attempted to explore the scope of some rules in current laws that could be used to govern it. Thus, the elements of theft offence (*actus reus*, property as a subject matter of theft and *mens rea*) were analysed in chapter four to scrutinise whether existing Iraqi theft offence laws are adequate to govern identity theft.[5] Iraqi Courts may encounter some difficulties when they attempt to apply these laws to identity theft. The study has determined these difficulties as below.

7.2.1.1 Difficulties Posed by the Element of Appropriation

The study's results showed that neither the Iraqi legislature nor the UK or the US legislature defines the term 'appropriation'. Therefore, scholars and judges have defined

[5] The *actus reus* refers to the appropriation of another person's property. The property as a subject of theft is the second element. To be subject to theft this property should belong to another person rather than the criminal. The term *mens rea* refers to the state of mind of the accused. It consists of two elements: dishonesty and the intention to permanently deprive the owner of his property.

it as the taking of or carrying another person's property away. By applying this definition to the unlawful obtaining of people's identities, the study found that the term 'appropriation' causes dissent between scholars and judges in relation to whether the act of appropriation could be considered as an element in an identity theft offence. Some legal scholars and professionals[6] believe that personal information cannot be a subject of taking or carrying away, whereas others[7] believe otherwise (the latter are of the view that the intangible materials could be taken or carried away through any means, which are deemed appropriate to its intangible nature). The author agrees with the first view, i.e., that personal information cannot be subject to physical taking or carrying away. The present study showed that therefore there is a gap in current theft offence laws with respect to the term 'appropriation' because it relies on the concept of 'taking and carrying'. This gap calls for legislative or judicial action to resolve it.

7.2.1.2 Difficulties Caused by the Application of the Term Property as an Element of Theft

In addition, the study analysed the definition of property used in existing Iraqi theft offence laws and explored the contention between scholars and judges as to whether a person's means of identification or financial information could be defined as 'property' and then be subject to theft. Some commentators argued that a person's means of identification or his financial information is property and it may therefore be subject to

[6] Clough pointed out in his article that confidential information cannot be taken or converted in a manner that resulted in the deprivation the victim, J Clough, 'Data Theft? Cybercrime and the Increasing Criminalization of Access to Data', (2011) Vol. 22 (1-2) Criminal Law Forum 145-170; Ricks stated that intangible property cannot be subject of conversion unless it is converted as well …. In addition, he stated that the trover action's basic assumed that the property involved must be bound up with tangible property, Val D Ricks, 'The Conversion of Intangible Property: Bursting the Ancient Trover Bottle with New Wine' (1991) Brigham Young University Law Review 1681-1715; *Dowling v United States* 473 US 207 (1985) in this case the court stated that the property should be a tangible thing and it should be taken by physical means, (such as taking or converting). It stated that personal information cannot be subject to theft because it cannot be taken by physical means.

[7] Ateek stated that stated that personal information is property and it can be subject to appropriation by any means irrespective whether the means is physical or non-physical (such as taking away, carrying away, seeing, or hearing), J Essegair, *Criminal Law and Modern Technology Crimes Arising from the Use of Computer* (1st edn Dar Al- Arabia Nahda 1992) 62; in the same vein Mahmoud stated that personal information cannot be cannot be subject to theft because it cannot be taken away or carried away by physical means, A Mahmoud, *Theft of the Stored Information in the Computer*, (3rd edn Dar Al-Arabia Nahda Cairo 2004) 297; *R. v. Offaly*. In this case, Ontario Court of Appeal held that personal confidential information is property and it may be a subject of theft. It stated that this information can be subject to taking or carrying away, *R. v. Offley* [1986] 28 C.C.C. (3d) 1

theft,[8] whereas others[9] argue that it is intangible and cannot satisfy the definition of property. Consequently, in their view it is not property. As a result, scholars and judges attempted to justify whether a person's means of identification or his financial information is property through considering the concept of property in terms of civil law provisions. To analyse the concept of property in civil law, the study referred to other rulings by the UK and US Courts because there is no case law on the point in Iraq, which may support the argument of the author. It has been shown that these foreign courts depend on two grounds to justify the conclusion that personal or financial information is property. The approach adopted by UK courts is called a 'breach of confidence and Contract or Equity approach' whereas US courts adopted the approach based on 'misappropriation or property theory and an equity or obligation approach'. The study showed that these attempts failed to provide an adequate basis that justifies a person's means of identification or their financial information as property. Therefore, the author suggests that the Iraqi legislature should mandate, in specific legislation, that personal and financial information of a person constitutes specific types of property.

7.2.1.3 The Consequence of the Analysing of the *Mens Rea* of Theft Offence

Continuing to investigate whether theft offence laws are adequate to govern identity theft, the study also discussed the difficulty that may be posed by the *mens rea* concept as an element of identity theft. It was highlighted how the *mens rea* constitutes an obstacle, which may interrupt and prevent the application of theft offence laws to identity theft. This obstacle is represented by the element of intention to permanently deprive the person of his means of identification or financial information. According to traditional theft offences, a person may be guilty of theft when he commits his crime with the intention of permanently deprive the owner of his property. According to the

[8] Kashkoush observed that personal information is property because it has a physical entity by which it can be viewed via a physical material, (such as a computer screen), H Kashkoush, *Computer Crimes in the comparative legislation* (Dar Al-Arabia Nahda Cairo 1992) 53; Jefferson pointed out personal information is property. He stated that if personal information is not considered property that will lead to anomalous consequences. It is unfair to consider a piece of paper contains expensive information as property, but the information is not, M Jefferson, *Criminal Law* (10th edn Pearson Education Limited London 2011) 603

[9] Hammond pointed out that personal information cannot be a subject of theft because it is intangible property, R.G. Hammond, 'The Misappropriation of Commercial Information in the Computer Age' (1986) Vol. 64 Canadian Bar Review 349- 52; Biograd stated that personal information is not property, particularly; that appears on a screen and it cannot be subject to theft, M Biograd, *Analysis Study of Theft and Appropriation, a Research Presented to the Six Conference of Egypt Group of Criminal Law*, (Cairo 1993) 372

above meaning of the *mens rea* of theft, the owner in theft offences is deprived of his property permanently, while the person involved in an identity theft offence is not deprived of his means of identification or financial information. He still uses them, as no permanent or even temporary appropriation has occurred. Consequently, the study has showed that the *mens rea* of identity theft does not fall within the concept of the scope of traditional *mens rea* (as it typically understood) of theft offences.

Given the above justification, the current study concluded that because of the forgoing difficulties, the current Iraqi theft offence laws are inadequate to govern identity theft. In other words, it has been concluded that identity theft does not fall within the scope of existing theft offences concepts. Consequently, this issue should be referred to either a competent court or the legislature so as to enact a new Act to deal specifically with identity theft.

7.2.2 The Role of the Iraqi Criminal Judge to Overcome the Previous Difficulties

The role of the judge to overcome the difficulties that are posed by the application of existing theft offence laws to identity theft has been analysed in chapter five. The author has attempted to examine the role of the Iraqi criminal judges and in reference to the judges in US and UK courts to overcome these difficulties through either extending the current theft offence laws, or creating new laws. The role of criminal judges to extend the current theft offence laws, or to create new laws may be achieved both by the interpretation of these laws, or analogy.

Having illustrated the interpretation of law and analogy issues, the thesis demonstrated how criminal judges could use three types of interpretation to interpret the ambiguous statute: the literal approach, the expansive approach and an interpretation that explores the spirit of the statute (the purposive approach). In the process of extending the current theft offence laws, or creating new laws, the study revealed that Iraqi criminal judges must abide by the contents of the criminal text when they attempt to interpret existing theft offence laws. In addition, it showed that those judges must interpret these laws in a manner that does not lead to extend the scope of them (creating crimes and setting out their punishments) or create new laws.

The majority of scholars believe that the best method that could be used to interpret the

law is the method that enables the judge to explore the legislature's intention when it enacted the law; irrespective of whether it is a literal or an expansive interpretation. Examining existing theft offence laws, the study proved that neither criminal judges in the Iraq nor the criminal judges in either the UK or the US could extend or create laws because the US and Iraqi systems contain the principle of legality that prevents criminal judges from creating laws; and the UK is upholding the convention of European Human Rights that prevents judges in the UK from creating new laws to govern new unlawful activities. The study showed the lack of judicial solution required the legislature in Iraq to find a legislative solution to overcome the inadequacy of theft offence laws.

Having examined the laws used to combat identity theft in both the US and UK, the study then showed that there are two different approaches that could be used by the US and the UK Courts to fight identity theft. The US has enacted two laws that deal with identity theft. Whereas the UK still suffers the lacuna in its legislation, and so the courts in the UK have resorted to many laws, such as the Data Protection Act, Theft Act 1968, Fraud Act 2006, and Computer Misuse Act 1990 to explore rules that could be used to protect a person's means of identification from illegal use with intent to commit other crimes. The Iraqi legislature may borrow or adopt provisions from either the UK or the US's approach or both. In the next section, the study will show whether the Iraqi legislature can borrow or adopt provisions from either the US or the UK's approach or both.

7.2.3 Borrowing or Adopting Provisions from Either UK or US Legislation or from Both

Both the current Iraqi theft offence laws and the Information Project of 2011 in Iraq are inadequate to deal with identity theft. In addition, the Iraqi criminal judges are incapable of overcoming what is absent in these laws: hence the legislature should enact a new law to address identity theft. In order to enact a comprehensive law to combat the identity theft offence, chapter six has attempted to examine whether the Iraqi legislature can adopt or borrow provisions from either UK or US legislation or both.

In Chapter six it was shown that the UK legislature does not consider identity theft as a separate crime; thus, it has not enacted a specific law to govern it. Therefore, the courts

in the UK have resorted to relying on a combination of many other laws, such as the Data Protection Act 1998, Theft Act 1968, Fraud Act 2006, and Computer Misuse Act 1990 to combat use of citizens' means of identification. These laws were analysed to examine whether the Iraqi legislature could borrow or benefit from their provisions.

Having analysed these laws, the study demonstrated that UK Courts have invoked the aforementioned range of laws, nevertheless, they have not classified the breaches as cases of identity theft *per se*, but rather (for example) in documentary fraud and obtaining property cases, that they were dealing with illegal acts that not judge the perpetrators for identity theft offences, but rather judged them for other crimes, such as fraud or obtaining property by deception.

The study demonstrated that UK laws are inadequate in this context dealing with identity theft. It was shown how the UK Theft Act 1968 suffers from the same previous flaws that the current Iraqi theft offence laws suffer. The study showed that the UK Data Protection Act 1998 is considered a regular Act rather that a criminal Act, because it contains civil and administrative provisions. Although the UK Fraud Act 2006 includes some provisions that can be used to combat sophisticated electronic methods, such as phishing and spam, the thesis demonstrated that this Act is still inadequate to cover all methods used to commit identity theft. Finally, the analysis of the UK Computer Misuse Act 1990 revealed that the Act was enacted to protect the integrity of the computer rather than the protection of citizens' information. This Act has some provisions to combat some sophisticated methods, such as hacking, but it is inadequate to curb identity theft at all.

Even though the UK laws have some shortcomings, the present study suggests that the Iraqi legislature can borrow and benefit from these provisions, to evaluate and amend Iraq's Fraud Offence Act 1969, to keep up with technological developments and curb modern crimes that come along with new technology. Iraq can also benefit from the introduction of these laws to enact a new law to challenge misuse of computers and to protect their integrity.

In chapter six, the author also attempted to analyse the new US identity theft laws to explore whether or not the Iraqi legislature could borrow or adopt provisions from the US legislation in order to challenge identity theft. By analysing the US identity theft

laws, the study showed that the US legislature does not criminalise the actual identity theft offence that takes place when a person takes another person's means of identification or his financial information without consent, with intent to commit other crimes. However, it criminalises the later stage, which is represented by the transfer of, use of, or possession of another person's means of identification or his financial information to commit other crimes.

The study showed that transfer of, use of, or possession of, another person's means of identification or his financial information does not constitute the *actus reus* of identity theft. The transfer of, possession of, or use of, another person's means of identification constitutes a preparatory act to commit other crimes. This preparatory act is called 'the use of stolen identity' to commit others crimes. Apart from the reasons and circumstances that invited the US legislature to criminalise the use of another person's means of identification or the possession of it (rather than criminalise the act of the unlawful obtaining of this means of identification), this study showed that the US's approach is a better approach to fight identity theft. Consequently, the Iraqi legislature can borrow provisions or benefit from US legislation[10] to fight identity theft, however, provided that Iraq avoids transplanting it with their flaws. In order to assist the Iraqi legislature to avoid the flaws found in the US's approach (identity theft laws), the current study has proposed recommendations that the Iraqi legislature can benefit from.

7.2.4 Recommendations

After examining the adequacy in existing Iraq theft offence laws and the adequacy of provisions of the Iraqi Information Crimes Project of 2011 to combat identity theft, the study showed that both are inadequate to govern identity theft offences. In order to overcome the inadequacy in theft offence laws, the study examined the role of criminal judges to scrutinise whether they can extend these laws (or create new laws) to govern identity theft and concluded that Iraqi judges could not.

[10] There are several provision were stated in both Identity Theft and Assumption Deterrence Act 1998 § 1028 (a) (7) and Identity Theft Penalty Enhancement Act 2004 US. The US legislature stated some elements of identity theft (such as transfer or using of another person's means of identification, the definition of a person's means of identification, and some elements of *mens rea*, such as without consent and contrary to the law). However, it does not criminalise the obtaining of this information which constitutes the actual identity theft. It considers the taking of this information with consent is identity theft, but the author observes it is not identity theft.

The thesis therefore suggests that the Iraqi legislature should enact a new law to govern identity theft. In order to assist the Iraqi legislature to enact the new law, this study suggests that the US identity theft laws are more suitable to be adopted by the Iraqi legislature. However, US identity theft laws cannot simply be transplanted or adopted in its current wording because there are many differences between both countries, such as culture, financial institutions organisation and practices, and their dealing with transactions and other elements that contribute to Iraqi society. They have also some flaws that should be avoided.

The recommendations that are presented by the thesis could be potentially workable and helpful to guide the Iraqi legislature to enact a comprehensive law to govern identity theft. If these recommendations are applied or adopted by the Iraqi legislature, they would be fruitful in preventing identity theft. Above all, these recommendations relate to the *definition of identity theft* and *its elements*. The Iraqi legislature should define identity theft and determine its elements (such as the *actus, reus* and *mens rea*) precisely.

The thesis has suggested a definition of identity theft as: a person is guilty of identity theft if he 'knowingly and willingly or recklessly and dishonestly, without consent obtains by any method whether sophisticated or not, personal or financial information of another person whether a legal entity or an individual person, transfers, sells, offers for sale, distributes, makes the use of this information available for others or uses this information for their own purposes.

With respect to the determination of the elements of identity theft, the study proposed some factors that the Iraqi should take into account. First, the study suggested that the Iraqi legislature should consider another person's means of identification as a type of property and then determine the meaning of it. The study has created a potential definition of means of identification. This study proposes that identification in the Iraq context should refer to 'any information whether biological or physiological that is usually used alone or combination with other information to identify or purport to identity a person'. The identity codes could include, but not be limited to fingerprints, voiceprint, retina or iris image, deoxyribonucleic acid (DNA) profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit

and debit cards numbers, financial institution account number, social security number, passport number, password and driver licence number.

This study has also suggested that the Iraqi legislature should consider the means of identification of both the legal entities and human persons as the subjects of identity theft. With respect to the individual's identity, the study suggested that the Iraqi legislature should state in the potential identity theft law that this means of identification belongs to the person who has a right to use it irrespective of whether the assumed identity is of a person who is dead or alive. In addition, it suggested that the Iraqi legislature should state that the abandoned means of identification of a person can be subject to theft if it used with the other current means of identification of that person with an intention to commit other crimes.

Secondly, the thesis suggested that the Iraqi legislature should determine precisely the *actus reus* of identity theft. The study has defined the *actus reus* of identity theft as: a person is guilty of identity theft if.

1. He knowingly and willingly or recklessly and dishonestly, without consent *obtains* another person's means of identification or their financial information.

2. Or after legally or illegally obtaining another person's means of identification, he knowingly and willingly or recklessly *uses* another person's means of identification or their financial information to commit other crimes, or aids or abets in the commission of these crimes.

3. If he transfers, sells, offers for sale, distributes, or makes the use of personal or financial information of another person available for others knowing that (or being reckless as to whether) such information would be or might be, used to commit a punishable crime.

In addition, the Iraqi legislature should consider some of the more sophisticated methods that are used to obtain personal or financial information of individuals, such as phishing, hacking, Trojan Horse or spam, which may be used later to commit other crimes, under aggravating conditions, or consider them as crimes in themselves.

Thirdly, the thesis also suggests that the Iraqi legislature should determine precisely the

mens rea of identity theft. The present study suggests that the *mens rea* of identity theft occurs when 'the accused knowingly and willingly and without another person's consent obtains or uses the means of identification of that person. The *mens rea* also takes place when the accused uses another person's means of identification without the person's consent irrespective of whether the use of this appropriated means of identification is permanent or temporary. In addition, the *mens rea* of identity theft takes place when the accused recklessly uses another person's means of identification.

The study has identified a potential definition refers to the meaning of both the *mens rea* and the *actus reus* of identity theft; namely, a person is guilty of identity theft if:

(1) He knowingly and willingly or recklessly and dishonestly, without consent *obtains* another person's means of identification or their financial information.

(2) Or after legally or illegally obtaining another person's means of identification, he knowingly and willingly or recklessly *uses* another person's means of identification or their financial information to commit other crimes, or aids or abets in the commission of these crimes.

(3) If he transfers, sells, offers for sale, distributes, or makes the use of personal or financial information of another person available for others knowing that (or being reckless as to whether) such information would be or might be, used to commit a punishable crime.

The use of the internet to commit identity theft makes the participation in the commission of the act more dangerous. Many perpetrators, either acting as separate individuals or as groups may also be involved in identity theft, thus the study suggests that the Iraqi legislature make provisions in the potential identity theft law to govern this kind of multiple participation in identity theft. These provisions may differ from those that govern other crimes. It should also consider identity theft as a global crime, and accede and ratify all related global conventions to extradite identity thieves to prosecute them. The current study proposes potential legal texts of participation in identity theft and call on the Iraqi legislature to adopt it - a person is guilty of participation in identity theft if he knowingly and willingly plans, commits identity theft, instigates, encourages, agrees with, orders another individual to commit identity

theft, or aids or abets in commission of identity theft.

In addition, this study suggests that the Iraqi legislature should consider some conditions as aggravating conditions, for example, but not limited to the use of the internet to commit identity, participating more than one person in committing it or inside workplace stealing a person's means of identification.

7.3 Suggestion for further Study

Studies show that identity theft is a fast growing crime in the world with devastating affects to many parties. Nowadays, the internet increases the faceless transactions where parties cannot meet each other face to face when they make their transactions, thus false impersonation is on the increase. In order to distinguish the real person from the impostor and then to prevent the commission of identity theft, it will be wise to further explore identity verification and its legal processes. In addition, verification types, and its 'modus operandi' to verify people may be subjects of future study.

Due to the internet connecting the whole world, identity theft can be committed remotely. The Commission of identity theft from inside one country against another country may give rise to the issue of the extradition and cooperation between States to extradite identity thieves and prosecute them. The extradition of identity thieves may also be subject to a future study.

7.4 Conclusion

This chapter demonstrated what has been achieved throughout this thesis. In this chapter the background of identity theft has been summarised. Then the author has briefly summarised the difficulties that may be faced if existing Iraqi theft offence laws applied to identity theft. The role of Iraqi judges to overcome these difficulties and find a solution to combat identity theft has been summarised in this chapter. The author also summarised in this chapter the issue whether Iraqi legislature can borrow a legislative solution that is demonstrated earlier in chapter six of this thesis. In addition, the author summarised some recommendations that he believes they may be useful to the Iraqi legislature when it intends to enact a new law to combat identity theft.

In nutshell, it is worth mentioning here that identity theft is a global crime, and is an

uncontrolled crime that can hit every country, irrespective of its advancement or under development in terms of technology. Thus, the fight against identity theft requires global cooperation between States. It needs cooperation between people within a given jurisdiction, as States' laws on identity theft crime *per se* are insufficient to curb identity theft. Public and private sectors including governments need to be educated on the techniques, cause, and consequences of identity theft. Companies and internet providers should also provide their computers by good programs of protection. In a more specific context, the Iraqi legislature should enact adequate laws that can effectively curb identity theft in all its tenets.

Bibliography

Books

Alraezki M., *Lecturers in Criminal Law, General Part, General Principles, a Crime and Responsibility*, (3rd edn, Dar Oya 2002)

Austin J, *Lectures on Jurisprudence* (1885) John Murray London

Ashworth A, *Principles of Criminal Law*, (6th Oxford University Press, United States, 2009)

Allen M J, *Textbook on Criminal Law* (8th ed, Oxford, Oxford University Press 2005)

Allen M J and Cooper S, *Elliot and Wood's Cases and Material on Criminal Law*, (10th edn, London, Sweet and Maxwell, 2010)

Al- Huseini A, *Important Problems in the Crimes Related to Internet and its International Dimensions*, (2nd edn, Dar Al- Arabia Nahda, without year)

Ateek, *Internet crimes*, (1st edn, Dar Al- Arabia Nahda, 2000)

Al-Qahwaji A, "*Criminal Protection of Computer Programs* (1992 Journal of Collage of Rights for the Economic and Law Research)

Al-Shawa M, The *Information Revolution and its Implications to the Penal Code*, (2nd edn, Dar Al-Arabia Nahda, 1998

Biegelman M T, *Identity Theft Handbook*: *Detection, Preventing, and Security* (2007)

Bloom W, *Personal Identity, National Identity and International Relations* (Cambridge Cob. V Press 1992)

Biograd M, *Analysis Study of Theft and Appropriation, a Research Presented to the Six Conference of Egypt Group of Criminal Law* (Cairo, 1993)

Bara M R, *General Principles of Libyan Penal Code*, (Khatraa Company 2010 K)

Curran K, Brisline P, and McLaughlin K, *Hacking and Eavesdropping,* (2008)

Chisholm H, *Encyclopaedia Britannica* (11th edn, Cambridge University Press, Cambridge, 1911)

Clarke R and Felson M, *Routine Activity and Rational Choice, (*London: Transaction Press, 1993)

Craats and Rennay, *Identity Theft: the Scary New Crime that Targets All of Us* (Toronto: Altitude Publishing, 2005)

Cherkassky L, et al, *Legal Skills* (Palgrave Mamillan 2011)

Cremona M, *Legal Method* (7th edn Palgrave Macmilan United Kingdom 2009)

Cole E and Ring S, *Insider Threat: Protecting the Enterprise from Sabotage, Spying and Theft*, (Elsevier / Syngress 2005)

Darbyshire P, *Darbyshire on the English Legal System* (10th edn Sweet Maxwell 2011)

Drake E, *50 Plus One Tips to Preventing Identity Theft*, Encouragement Press, L L C, 1261, W.Glenlake, Chicago IL.60660

Deng F, *War of Vision Conflict of Identities in the Sudan*, (Washington DC: Brooking 1995)

Elliott C and Quinn F, *Criminal Law*, (8th edn, London, Hinry Ling Ltd, Dorset Press, Dorset, 2010)

Elliott C and Quinn F, *English Legal System* (11th edn Pearson Education Limited London 2010)

Essegair J, *Criminal Law and Modern Technology, Crimes Arising from the Use of Computer, (*First edition, Dar Al- Arabia Nahda 1992)

Ferri E, *Criminal Sociology*, 227, (D. Appleton & Co. 1897)

Ghannam K, *Traditional Rules in Penal Code Are Insufficient to Combat Computer Crimes*, (Emirates University, 2000)

Gillespie A, *The English Legal System* (2nd edn Oxford University Press 2009)

Lyle Helen M., *Jack Cade's Rebellion 1450*, (George Philip & Son, Ltd., Historical Association 1950)

Hogg M and Abrams D, *Social identification: A Social Psychology of Intergroup Relations and Group Processes*, (1st edn, Routledg London: 1988)

Heaton R, *Criminal Law*, (2nd edn, Oxford University Press, 2009)

Hosni M, *Penal Code Explain, Private Section*, (Dar Al-Arabia Nahda, Cairo, 1994)

Huxley-Binns R and Martin J, *Unlocking the English Leagal System* (3rd edn Hodder Education 2010)

Herring J, *Criminal Law*, (7th edn, Palgrave Mcmillan Law Masters UK 2011)

Herring J, *Criminal Law: Text Cases and Materials* (4th edn Oxford University Press 2010)

Jefferson M, *Criminal Law* (8th edn Pearson Education Limited Edinburgh 2007)

Jefferson M, *Criminal Law* (9th edn Pearson Education Limited England 2009)

Jefferson M, *Criminal Law*, (10th edn, Pearson Education Limited London 2011)

Kashkoush Huda, *Computer Crimes in the comparative legislation*, (Dar Al-Arabia Nahda, Cairo, 1992)

Molan M T, *Cases G Materials on criminal law* (3rd edn London: Cavendish 2005)

Mahmoud A, *Theft of the Stored Information in the Computer* (3rd edn, Dar Al-Arabia Nahda, Cairo, 2004)

Mallach A, *Bringing Buildings Back*: *From Abandoned Properties to Community Assets*, (Rutgers University Press, 2005)

Mcleod I, *Legal Method*, (7th edn, Palgrave Macmillan England 2009)

Mustafa M M, *Penal Code Explaining*, (Cairo, 1974)

Newman G R and Clarke R, *Superhighway robbery: Preventing e-commerce crime* (London: Willan, 2003)

Newton J, Det. Chief Insp *Organized Plastic Counterfeiting* London (Home Office 1994)

Nimmer R, *The Law of Computer Technology* (3rd edn, 1997)

Ormerod D, *Smith and Hogan, Criminal law* (12th edn OUP Oxford 2008)

Ormerod D, *Criminal Law, Cases and Materials* (10th edn Oxford University Press New York 2009)

Ormerod D, *Smith and Hogan's Criminal Law* (13th edn Oxford University Press 2011)

Oxford English Dictionary, (2nd edn 1989)

Merriam-Webster Online Dictionary available at <http/www.m w.comdictionary/identity> viewed on Jul 25, 2010

Ramadan U, *Penal Code explains*, *Specific Section*, (Dar Al-Arabia Nahda, 1986)

Reed A and Fitzpatrick B, *Criminal Law*, (4th edn, Sweet and Maxwell Limited, 2009)

Rustom H, *Penal Code and the Dangerous of Information Technology*, (Modern Tools Library, without published year)

Reed C and Angel J, *Computer Law: The Law and Regulation of Information Technology*, (6th ed, Oxford University Press, New York, 2007)

Rashid A and Ali BA, *An Explanation of the General Theories of Criminal Law* (Dar Al-Arabia Nahda Cairo 1972)

Simester A and Brookbanks W, *Principles of Criminal Law* (3rd edn, Thomsons Brookers, Wellington, 2007)

Simester A P, Spencer J R, Sullivan G R and Virgo G J, *Simester and Sullivan's Criminal Law, Theory and Doctrine* (4th edn Oxford and Portland, Oregon 2010)

Shawabkeh M, *Computer and Internet Crimes, Cyber Crime*, (Dar Al-Thaqafa, Amman, 2004)

Singer R G and Fond JQ La, *Examples and explanations: Criminal law* (5th edn, Aspen Publisher New York 2010)

Shamuon A, *The National Plan for Human Rights- The Right in Living, Lebanon Parliament Council* (without a year publishing)

Soruor A F, Al- Waseet in Criminal Law, (6th edn, Dar Arabic Nahda, Cairo 1996)

Tenney M C, ed, *The Zondervan Pictorial Bible Dictionary*, (Grand Rapids, MI: Zondervan Publishing House1969)

Tonry M, *The Oxford Hand Book of Crime and Public Policy* (New York Oxford University Press 2009)

Tammam A, *Crimes Related to Internet Use, Comparative Study*, (1st edn, Dar Al-Arabia Nahda, Cairo, 2000)

Weisdurd D, Waring E and Chayet W E F, *White-Collar Crime and Criminal Careers*, (Cambridge, UK, Cambridge University Press 2001)

Wilson W, *Criminal law: Doctrine and Theory*, (2nd edn London: Longman 2003)

Ward R and Akhtar A, *English Legal system* (11th end, Oxford University Press Inc. New York 2011)

Zander M, *The Law Making – Process* (6th edn Law in Context CUP Cambridge 2004)

Articles

Allison S, M Schuck A and Lersh K M, 'Exploring the Crime of Identity Theft: Prevalence, Clearance and Victim /Offender Characteristics'. (2005) (33) Journal of Criminal Justice

Angelopoulou O, Thomas P, Xynos K, and Tryfanos T, 'On-line ID Theft Techniques, Investigation and Response, Information Security Research Group' (2007) Vo. 1 (1) Int. J. Electronic Security and Digital Forensics

Awad N F and Fitzgerald K, 'The Deceptive Behaviours That Offend US Most about Spyware' (2005) Vo. 48 (8) Communications of the ACM

Arias A V, 'Life, Liberty, and the Pursuit of Swords and Armor: Regulating the Theft of Virtual Goods' (2008) Vo.57 Emory Law Journal

August R, ‘International Cyber-Jurisdiction: A Comparative Analysis’ (2002) Vol. 39 American Business Law Journal

Berry M R, ‘Does Delaware’s Section 102(b) (7) Protects Reckless Director from Personal Liability? Only if Delaware Courts Act in Good Faith’ (2004) Vol.79 Law Journal Library Washington Law Review

Branner S W, ‘Is There Such a Thing as “Virtual Crime”?’ (2001) Vol.4 (1) California Criminal Law Review

Buba Nicole M, ‘Wagin War Against Identity Theft: Should the United States Borrow from the European’s Union Battalion?’ (1999-2000) 23 Suffolk Transnat'l L. Rev.

Bernstein Susan E, ‘New Privacy Concern for Employee Benefit Plans: Combating Identity Theft’ (2004) Vol.36 (1) Compensation and Benefits Review

Brooke A Masters and Caroline E, Mayer, ‘Identity Theft More Often an Inside Job, Newsbytes News Network’ Dec. 3, 2002 cited in E L Sylvester, ‘Identity Theft: are the Elderly Targeted’ (2004) Vol. 3 (2) Connecticut Public Interest Law Journal

Chawki M and Abdel Wahab S, ‘Identity Theft in Cyberspace: Issues and Solutions’ (2006), Vol. 11 (1) Lex Electronica

Bainbridge D, ‘Criminal Law Tackles Computer Fraud and Misuse’ (2007) Vol. 23 (3) Computer Law & Security Report

Clough B and Mango P, ‘Companies Vulnerable to Identity Theft’ (2003) AFP Exchange) Vol.23 (4)

Conry-Murry A, ‘Who Knows What Evil Lurks?’ (2006) Vol. 21 (3) IT Architect

Campbell K, ‘The Test of Dishonesty in *R .v. Ghosh*’ (1984) Vol. 43 Cambridge Law Journal

Charlesworth A, ‘The Future of UK Data Protection Regulation’ (2006) Vol.11 (7) Information Security Technology Report

Cradduck L and McCullagh A, ‘Identifying the Identity Thief: Is It Time for a (Smart) Australia Card’ (2007) Vo. 16 (2) international Journal of Law and Information Technology, Oxford University Press

Christie A L, ‘Should the Law of Theft Extend to Information?’ (2005) Vol. 69 Journal of Criminal Law

Clough J, ‘Data Theft? Cybercrime and the Increasing Criminalization of Access to Data’ (2011) Vol. 22 (1-2) Criminal Law Forum

Cross J T, ‘Protecting Confidential Information under the Criminal Law of Theft and Fraud’ (1991) Vo. 11 (2) Oxford Journal of Legal Studies

Coleman A, ‘Trade Secrets and the Criminal Law in Canada’ (1988) Vol. 10 (1) Eur. Intell. Prop. Rev.

Cross J, ‘Trade Secrets, Confidential Information, and the Criminal Law’ (1991) Vol. 36 McGill, L.J.

Conradi M, ‘Legal Development in IT Security’ (2007) Vol. 23 (4) Computer Law & Security Report

Christian C, ‘Down and Out in Cyberspace’ (1993) 90 L S Gaz

Charlesworth A, ‘Legislating Against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990’ (1993) Vol. 4 (1) Journal Law & Information Science

Diedrich B, ‘Chapter 254: Closing the Loopholes on Identity Theft, But at What Cost?’ (2002) Vol.34 McGeorge Law Review

Dwan B, ‘Identity theft’ 2004’, Vol. 2004 (4) Computer Fraud and Security

Davies C R, ‘Protection of Intellectual Property –A Myth? A Consideration of Current Criminal Protection and Law Commission Proposals’ (2004) Vol. 68 Journal of Criminal Law

Dana S, ‘Criminal Law Beyond Retroactivity to Realizing Justice: A Theory on the Principle of Legality in International Criminal Law Sentencing’ (2009) Vol. 99 (4) The Journal of Criminal Law & Criminology

Dunnill R and Barham Ch, ‘Confidentiality and Security of Information’ (2007) Vol.8 (12) Anaesthesia and Intensive Care Medicine

N Dunne, ‘ID Theft for Beginners’ (2008) Vol. 2008 (1) Network Security

Edwards L, ‘Down of the Death of Distributed Denial of Service: How to Kill Zombies’ (2006) Vol. 24 (23) Cardozo Arts & Entertainment,

Endeshaw A, ‘Theft of Information Revisited’ (1997) Vol.187 Journal of Business Law

Fairfield Joshua A.T, ‘Virtual Property’ (2005) Vo. 85 Boston University Law Review

Franks C W, ‘Comment Analyzing the Urge to Merge: Conversion of Intangible Property and the Merger Doctrine in the Wake of *Kremen v Cohen’* (2005-2006) Vol. 42 (489) Houston Law Review

Frankland J, 'Numeric Data Integrity: Piercing the Corporate Veil' (2009) Vol. 2009 (8) Network Security

Flanagan A, 'The Law and Computer Crime: Reading the Script of Reform' 2005 Vol.13 (1) International Journal of Law & Information Technology

Fontana J, 'Rootkits Aren't Doom But Keep up Defences' (2006) Vol. 23 (16) Network World

Ford R, 'Malware Briefing' (1998) Vo.17 (2) Computer and Security in D B Owen, 'The State of Malware' (without year) 10 available at <http://danielowen.com/files/The_Stae_of_Malware.pdf > accessed on 3 November 2010

Green S P, 'Why It's a Crime to Tear the Tag off a Mattress: Overcriminalization and the Moral content of Regulatory offences' (1997) Vo. 46 (4) Emory Law Journal

Gordon G.R and, Willox N.A, 'Identity fraud: A Critical National and Global Threat' (2004) Vo. 2 (1) Journal; of Economic Crime Management

Green S P, 'Moral Ambiguity in White Collar Criminal Law' (2004) Vol. 18 Notre Dame Journal of Law Ethics and Public policy

Gerard G, Hillison W, and Pacini C, 'What Your Firm Know about Identity Theft' (2004) Vol. 15 (4) Journal of Corporate Account and Finance

Garie D B and Wong R, 'Parasiteware: Unlocking Personal Privacy' 2006 Script-ed, Vo. 3 (3)

Green S P, 'Plagiarism, Norms, and the Limits of Theft Law: Some Observations on the Use of Criminal Sanctions in Enforcing Intellectual Property Rights' (2002) Vol. 54 Hastings Law Journal

Carrier Michael A and Lastowka G, 'Against Cyberproperty' (2007) Vol. 22 Berkeley Technology Law Journal

Gringras C, 'To Be Great is to Be Misunderstood: the Computer Misuse Act 1990' (1997) Vol. 3 (5) Computer and Telecommunications Law Review

Gercke M, 'Project on Cybercrime, Internet-related Identity Theft,' A Report has been Prepared within the Framework of the Project on Cybercrime of the Council of Europe as a Contribution to the Conference "Identity Fraud and Theft – the Logistics of Organised Crime"' (2013) available at

<http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf> accessed on 22 May 2013

Heller I., 'How the Internet Has Expanded the Threat of Financial Identity Theft, and What Congress Can Do to Fix the Problem' (2008) Vol. XVII: 1Kansas Journal of Law & Public Policy

Hoofing Ch., 'Identity Theft: Making the Known Unknowns Known' (2007) Vol.21 (1) Harvard Journal of Law & Technology

Hoar S, 'Identity Theft: the Crime of the New Millennium' (2001) Vo. 80 (4) Oregon Review

Hayes F, 'Routed by Rootkits' (2006) Vol. 40 (16) Computer World

Henry P A, 'Firewall Considerations for the IT Manager' (2005) Vol.14 (5) Information System Security in D B Owen, 'The State of Malware' (without year) 10 available at <http://danielowen.com/files/The_Stae_of_Malware.pdf > accessed on 3 November 2010

Hilley S 'Police Catch UK Phisher' 2004 Vo. 2004 (5) Computer Fraud and Security

Hamdorf K, 'The Concept of Joint Criminal Enterprise and Domestic Modes of Liability for Parties to a Crime' (2007) Vol. 5 Journal of International Criminal Justice

Hammond R.G, 'The Misappropriation of Commercial Information in the Computer Age' (1986) Vol. 64 Canadian Bar Review

Hammond R.G., 'Theft of Information' (1984) 100 L.Q. Rev

Hiti M, 'Difficulties That May Obstruct the Application of Iraqi Theft Offence Laws to Crimes against Computer Programs' (2004) Journal of Sharia and law, United Arab Emirates

Hammond R G, 'Is Breach of Confidence Properly Analysed in Fiduciary Terms?' (1979) Vol. 25 McGill Law Journal

Hammond R G, 'Quantum Physic, Econometric Models and Property Right to Information' (1981) Vol. 27 McGill Law Journal,

Hall J, Nulla Poena Sine Lege (1937) Vol. 47 (2) Yale Law Journal

Hinde S, 'Knowledge is Power: Protecting Privacy' (2005) Vol. 2005 (7) Computer Fraud and Security Information System Security

Ingram D M, 'How to Minimize Your Risk of Identity Theft' (2006) Vol. 77 (6) Optometry, Journal of the American Optometric Association

InsuWhang, ‘The Property Concept in Criminal Law’ Dissertation of Sungkyunkwan University (2006)

Jennifer L, ‘Identity Theft, in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attack’ (2005) Vol. 20 Berkeley Law Journal

Jenkins R, ‘Categorization: Identity, Social Process and Epistemology’ (2000) Vol. 48 (3) Current Sociology

Katyal N K, ‘Criminal Law in Cyberspace’ (2001) Vol.149 University of Pennsylvania Law Review

Koops B J & Leenes R, ‘ID Theft, ID Fraud/or ID Related Crime. Definitions Matter’ (2006) Vo. 30 (9) Datenschutz und Datensicherheit

Krebs B, ‘Joint Criminal Enterprise’ (2010) Vol. 73 (4) The Modern Law Review

Lacey D and Cuganesan S, ‘the Role of Organizations in Identity Theft Response: Organization-individuals Dynamic’ (2004) Vol. 38 (2) The Journal of Consumer Affair

Lopucki L, ‘Did Privacy Cause Identity Theft?’ (2002-2003) Vol. 54 (4) Hasting Law Journal1

Lanham D, ‘Accomplices, Principals, and Causation’ (1979) Vol. 12 Melbourne University Law Review

LoPucki L M, ‘Human Identification Theory and the Identity Theft Problem’ (2001) Vol. 80, Taxes Law Review

Lynch J, ‘Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks’ (2005) Vol. 20 Berkeley Tech. J.L

Lawton G. ‘Virus Wars: Fewer Attacks, New Threats’ (2002), Computer, Vol. 35 (12) Technology news, IEEE Xplore

Lipton J D, ‘Mixed Metaphor in Cyberspace: Property in Information and Information Systems’ (2003) Vol.35 (1) Loyola University of Chicago Law Journal

Li L, ‘Nulla Poena Sine Lege in China: Rigidity or Flexibility?’ 2010) Vol. 43 (3) Suffolk University Law Review

Lamb S, Nullum Crimen, ‘Nulla peona Sine Lege in International Criminal Law in the Rome Statute of the International Criminal Court: A Commentary’ (Antonia Cases, Paola Gaeta & John R. W. D. John eds., 2002)

McGowan D, ‘The Trespass Trouble and the Metaphor Muddle’ (2005) Vol. 1 (200) Journal of Law, Economics & Policy

McCutcheon M C, ‘Identity Theft, Computer Fraud and 18 U.S.C § 1030(g): A Guide to Obtaining Jurisdiction in the United States for a Civil Suit against a Foreign National Defendant’ (2001) Vol. 13 (1) Loyola Law Review

McLaughlin L, Bot Spyware Spread, Causes New Worries, (2004) Vol. 5 (6) IEEE Distributed systems online, IEEE Computer Society

Marcus P, ‘Joint criminal Participation Establishing Responsibility, Abandonment Law in U S A Faces Social and Scientific Change, Section V’ (1986) Vol. 34 American Journal of Comparative Law Supplement

Motivate F and Tremblay p, ‘Counterfeiting Credit Cards: Displacement Effects, Suitable Offenders, Crime Waves Patterns’ (1997) Vol. 37 (2) British Journal of Criminology

Moohr G S, ‘Federal Criminal Fraud and the Development of Intangible Property Rights in Information’ 2000, Vo. 2000 University of Illoins Law Journal

Macpherson L, ‘Theft of Information’ (1994) Vol. 63 (3) Scottish Law Gazette

Marron D, ‘Alter Reality: Governing the Risk of Identity Theft’ (2008) Vol. 48 British Journal of Criminology

Mulhall T, ‘Where Have all the Hackers Gone? Part 4- Legislation’ (1997) Vol. 16 (4) Computer Law & Security Report

Nehaluddin A, ‘Hacker’s Criminal Behaviour and Laws Related to Hacking’ (2009) Vol. 15(7) Computer and Telecommunications Law Review

Parisi R, ‘Identity Theft: A Fast Growing Problem’ (2007) Vo. 2 (1) Risk Intelligence

Pritchett C. Herman, ‘The Roosevelt Court: A Study in Judicial Politics and Values’ 1937-1947(Macmillan 1948)

Perl M W, ‘It’s not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft’ (2003) Vo. 94 (1) the Journal of Criminal Law & Criminology.

Provenza Kristen S, ‘Identity Theft: Prevention and Liability’ (1999) Vol. 3 North Carolina Banking Institute

Ricks Val D, ‘The Conversion of Intangible Property: Bursting the Ancient Trover Bottle with New Wine’ (1991), Brigham Young University Law Review

Rumbles W, ‘Theft in the Digital: Can You Steal Virtual Property?’ (2011) Vol. 17 (2) Canterbury Law Review

Robinson P H, ‘Fair Notice and Fair Adjudication Two Kinds of Legality’ (2005) Vol. 154 University of Pennsylvania Law Review

Stuhlmiller N J, ‘Flores-Figueroa and the Search for Plain Meaning in Identity Theft Law’ (2010) Vol. 58 Buffalo Law Review

Sprague R and Ciocchetti C, ‘Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws’ (2009) Vol. 19 (1) Albuquerque Law Journal Science& Technology

Swartz N, ‘Will Red Flags Detour ID Theft?’ (2009), Vol. 43(1) Information Management Journal

Saunders K M and Zucker B, ‘Counteracting Identity Fraud in the Information Age: the Identity Theft and Assumption Deterrence Act’ (1999) Vol. 8 Cornel Journal of Law and Public Policy

Sylvester E L, ‘Identity Theft: Are the Elderly Targeted’ (2004) Vo. 3 (2) Connecticut Public Interest Law Journal

Steel A, ‘The True Identity of Australia Identity Theft Offences: A Measured Response or Unjustified Status Offences?’ (2010) Vol. 33 (2) UNSW Law Journal

Schreft, S L ‘Risks of Identity Theft: Can the Market Protect the Payment System’ (2007), fourth quarter, Economic Review Federal Reserve Bank of Kansas

Sipior J C, Ward T, and Rosell R, ‘The Ethical and Legal Concerns of Spyware’ (2005) Vol.22 (2) Information Systems Management in D B Owen, ‘The State of Malware’ (without year) 10 available at <http://danielowen.com/files/The_Stae_of_Malware.pdf > accessed on 3 November 2010

Stafford T F and Urbaczewski A, ‘Spyware: the Ghost in the Machine’ (2004) Vo. 14 (2004) Communications of the Association for Information Systems

Suri P and Rani S, ‘Security Manager- Key to Restrict the Attack in Bluetooth’ (2007) Vol. 3 (7) Journal of Computer Science

Shukla S and Nah F F, ‘Web Browsing and Spyware Intrusion’ (2005) Vol. 48 (8) Communications of the ACM

Smith J C, ‘Criminal Liability of Accessories: Law and Law Reform’ (1997) 113 Law Quarterly Review

Swartz N, ‘Want the CIA Director’s Address? Get It for $26 Online’ (2003) Vol.37 (6) Information Management Journal

Steel A, ‘Problematic and Unnecessary? Issues with the Use of Theft Offence to Protect Intangible Property’ (2008) Vol. 30 Sydney Law Review

Samuelson P, ‘Is Information Property?’ (1991) Vol. 34 (3) Communication of the ACM

Stuckey J E, ‘The Equitable Action for Breach of Confidence: Is Information Ever Property?’ (1982) Vol. 9 Sydney Law Review

Samuelson P, ‘Information as Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?’ (1989) Vol. 38 (2) Catholic University Law Review

Shahabuddeen M, ‘Does the Principle of Legality Stand in the Way of Progressive Development of Law?’ (2004) Vo. 2 (4) Journal of International Criminal Justice

Schaack B Van, ‘the Principle of Legality in International Criminal Law’ 2009 Vol. 103 (1) American Society of International Law

Stuntz William J, ‘The Pathological Politics of Criminal Law’ (2001) Vol. 100 Michigan Law Review

Savirimuthu A and Savirimuthu J, ‘Identity Theft and System Theory: The Fraud Act 2006 in Perspective’ (2007) Vol. 4 (4) Scripted 440 available at <http://www.law.ed.ac.uk/ahrc/script-ed/vol4-4/savirimuthu.pdf> accessed on 15 July 2012

Síthigh Daithí Mac, ‘Law in the Last Mile: Sharing Internet Access Through WiFi’ 2009 Vol. 6 (2) Scripted available at <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-2/macsithigh.pdf> viewed on 15 July 2012

Sumroy R ‘Computers: Computer Misuse and Data Protection’ (1997) Computer and Telecommunications Law Review

Stein K, ‘"Unauthorised Access" and the U.K. Computer Misuse Act 1990: House of Lords "leaves no room" for ambiguity’ (2000) Computer and Telecommunications Law Review

Sullins Lauren L, ‘Phishing for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft’ (2006) Vol. 20 (1) Emory International Law Review

Singleton S, ‘Comment Computer Misuse Act 1990-Recent Developments’ (1993) Vol. 57 Journal Criminal Law

Thomson R, ‘Why Spyware Poses Multiple Threats to Security’ (2005) Vo.48 (8) Communications of the ACM

Victor Gary M, ‘Identity Theft, Its Environment and Proposal for Change’ (2006) Vol. 18 (3) Loyola Consumer Law Review

White M D, ‘Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts’, (2008), Vol. 19 (1) Criminal Justice Policy Review

Wales E, ‘Identity Theft’ (2003) Vol. 2003 (2) Computer Fraud & Security

Wilkins S, ‘Criminal Law-Accomplice Liability’ (2007) Vo. 85University of Detroit Mercy Law Review

Weiss A, ‘Spyware Be Gone!’ (2005) Vo.9 (1) Networker

Wendt A, ‘Anarchy Is What State Make of It’ (1992) Vol. 46 (2) International Organizations

Wendt A, ‘Collective Identity Formation and the International State’ (1994) Vol. 88 (2) American Political Science Review

Willox N A., Jr. and Regan T M, ‘Identity Fraud: Providing a Solution’ (2002) Vol.1 (1) Journal of Economic Crime Management1

Tetley W, ‘Mixed Jurisdictions: Common Law v. Civil Law (Codified and Uncodified)’ (2000) Vol. 60 (3) Louisiana Law Review

Weinrib A S, ‘Information and Property’ (1988) Vol. 38 (2) University of Toronto Law Journal

Withey C, ‘Comment: The Fraud Act 2006- Some Early Observation and Comparison with Former Law’ (2007) Vol. 71 Journal of Criminal Law

Wasik M, ‘The Computer Misuse Act 1990’ Vol. (1990) Criminal Law Review

Walton R, ‘The Computer Misuse Act’ (2006) Vo. 1 (1) Information Security Technological Report

Yar M, ‘Computer Hacking: Just Another Case of Juvenile Delinquency?’ (2005) Vo. 44 (4) The Harvard Journal

Lee Y and Kozar K A, Investigating Factors Affecting the Adoption of Anti-spyware System (2005) Vo.48 (8) Communications of the ACM

Zaidi K, Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada’ (2007) Vol. 19 (2) Loyola Law review

Zhang X, 'What Do Consumers Know about Spyware?' (2005) Vo.48 (8) Communications of the ACM

Table of Cases

Chapter one cases

Oxford v. Moss [1979] Crim LR 119 DIVQBD

K and *Others v Criminal Court First Degree*, Dubai Courts, Criminal 5 (2004) [2004]

Chapter two cases

United States v. Blixt, 548 F. 3d 882 C.A.9 (Mont.), 2008

Oxford v Moss [1979] Crim LR 119 DIVQBD

United States v. Godin 534 F. 3d 51; 2008 U.S. App. Lexis 15301

United States of America v. Landy Diaz, No. 10-4305, (United States Court of Appeal Fourth Circuit, 2011) unreported

United States of America v. Brown, No 10-3170, United States Court of Appeal, (3rd Cir. 2011) unreported

TRW, Inc v Andrews, 534, United States Supreme Court, 19, (2001)

Chapter three cases

United States of America v. Corey L. Hines, United States Court of Appeals, 472 F. 3d 1038 (8th Cir. 2007)

U. S. v. Williams 355 F.3d 893, 2003 Fed.App. 0453P

United States of America v. Karen Battle, United States Court of Appeals, No. 10.1984 (3rd Cir. 2011) unreported

Krottner v. Starbucks Corp, United States Court of Appeals, 628 F. 3d 1139 (2010) Nos. 09-35823, 09-35824 (9th Cir. 2010)

United States of America v. Karen Clark, United States Court of Appeals, No. 10-10801 (11th Cir. 2011) unreported

United States of America v. Thomas Dale Peterson, United States Court of Appeals, 353 F.3d 1045(9th Cir. 2003)

United States of America v. April Nicole Garret, United States Court of Appeals, Fourth Circuit , No. 08-4933 (2011) unreported

California v Greenwood, Supreme Court of United States, 486 U.S. 35 (1988)

United States of America, v. Gustavo Villanueva-Sotelo, United States Court of Appeals 515 F. 3D 1234 (2008)

Williams v Phillips, Division Court (1957) 41 Cr. App. R. 5; (1957) 121 J. P. 163

United States v. Todd A. Wills, United States Court of Appeals, No. 06-6009 (10th Cir. 2007) unreported

United States v. Marry L. Landrry, United States Court of Appeals, No. 09-1877 (1st Cir. 2011) unreported

United States v. Michael F. Kimble, Sr., No.02-CR-549-A (E.D. Va.), July 17, 2003 (*U.S. v. Kimble*, 70 Fed. Appx. 113 C.A.4 (Va.), 2003)

United States v. Abdelshafi, United States Court of Appeals, 592 F. 3d 602 (4th Cir. 2010)

United States v. Bush, United States Court of Appeals, 404 F. 3d 263 (4th Cir. 2005)

United States v. Gonzalez, United States District Court, District of New Jersey, No. 09-10382-DPW (2009) unreported

United States v. Wallace L. Lawrence, United States Court of Appeals, Tenth Circuit, No. 10-6257 (D.C.No. 5:10-CR-00011-D-1) (W.D.Okla.) (2011) unreported

Federal Trade Commission v Zachary Keith Hill, United States District Court Southern District of Texas N. H 03-5537 (2004) unreported

United States v. Stepanain, United States Court of Appeals, No. 08- 1053 (1st Cir. 2011) unreported

U.S. v. Albert Gonzalez, U.S. District Court in Massachusetts, No. 08-10223 (2009) unreported

United States of America v. Shephard, United States Court of Appeals, No. 10-3215 (8th Cir. 2011) unreported

R v Allan [1963] 2 All ER 897, Court of Criminal Appeal

R v Clarkson and Carroll [1971] 3 All ER 344, Courts-Martial Court

United States v. Lyons, United States Court of Appeals, No. 07-3216 (8th Cir. 2009) unreported

United States of *America v. Bell*, United States District Court, Pennsylvania, No. 09-672 (2011) unreported

United States v. Garguilo, 310 F .2d 249, 254 (2nd Cir. 1962)

Rv.Bryce, (2004) EWCA crime 1231 and crime (2004) LR 936

United States of America v. Oliver, United States Court of Appeals, No. 09-10133 (5th Cir. 2011) unreported

Michigan v. Poplar, 173, N, W. 2d 732 (1969)

United States of America v. Damache, United States District Court for Eastern District of Pennsylvania, No. 11-420 (2011) unpublished

Johnson v. Youden (1950)1 All ER 300

United States of America v. Abdullatif Jabi, United States Court of Appeals, No. 90-3643 (6th Cir. 2011) unpublished

United States of America v. Karen Clark, United States Court of Appeals, No. 10-10801 (11th Cir. 2011) unreported

United States of America v. T Kasenge, United States Court of Appeals, [1st Cir. 2011] unreported

Minnesota v. St. Christopher 232 N.W .2d 789 (1975)

United States v. Bruno 105 F .2d 921 (2nd Cir. 1939), rev'd on other grounds, 308 U.S. 281

United States of America v. Gonzales, United States District Court, District of New Jersey, No. 09-18 U.S.C. §371 and 1349 (2009) unreported

United States of America v. Berdize, United States Court of Appeals, No. 10-0064 Cr, [2nd Cir. 2011]

Direct Sales Co. v. United States 319 U. S 703(1943)

Pin Kenton v. United States 328, U.S. 640 (1946)

R v Powell and English, (1999), 1 AC1 (HL)

Harris v Harrison [1963] Crim LR497, DC.cf Williams CLGP, 322

United States of America v Roperto Miranda- Lopez, United States Court of Appeals, No 07-50123 (9th Cir. 2008) unreported

Flores –Figueroa v United States, United States Court of Appeals, 129 S Ct 1886(8th Cir. 2009)

States of Kansas v. Bradly D Hardesty, Court of Appeal of the States of Kansas, 42 Kan. App. 2d 431 (2009)

United States v. Ozuna Carbera, United States Court of Appeals 663 F. 3d 496 (1st Cr. 2011)

Chapter four cases

United States v. Bottone, (1966) 356 F.2d 389, cert denied, 385 U.S 974, 6

Dowling v United States 473 US 207 (1985)

United States v. Ochs 842 F.2d 515, 521 (1st Cir. 1988)

United States v Brown, 925 F2d 1301, 1308-09 (10th Cir. 1991)

McNally v. United States, 483 U.S. 350 (6th Cir. 1987)

United States v. Gimbel 830 F.2d 626, 627 (7th Cir. 1987)

Oxford v Moss [1979] 68 Cr App Rep 183

R v. Stewart [1988] 1 SCR 963

R v, Stewart [1983] 42 O.R. (2d) 225; 149 D. L. R (3d) 583

R v Offley [1986] 28 C.C.C. (3d) 1

R .v. Offley 1986), 70 A.R. 365

United States v. Seidliz, 589 F.2d 152 (4th Cir. 1978)

United States v. Cherif 943 F.2d 692 (7th Cir. 1991)

United States v. Czubinski 106 F.3d 1069, 1074 (1st Cir. 1997)

United States v. Carpenter, 484 U.S. 19, 108 S.ct. 316, 98 (1987)

C Schweppes Inc v. FBI foods Ltd [1999] 1 SCR 142

International News Service v. Associated Press, 248 U.S. 215 (1918)

Chiarella v. United States, 445 U.S. 222 (1980)

Robinson v. Brier 194, A. 2d 204, (Pa. 1963)

Franco v. J.D. Street & Co. 360 S.W. 2d 597(Mo. 1962)

Gaynor v. Buckley 203 F. Supp. 620 (Dist. Court D. Oregon. 1962)

Irving Trust Co. v. Deutsch 73 F.2d 121(2nd Cir. 1934)

Seager v Copydex Ltd [1967] 1 WLR 923

Coco v. Clark [1969] RPC 41

The Case of Swans (1572–1616) 7 Co Rep 15b

Blades v Higgs (1865) 11 HLC 621, 11 ER 1474, 628

R v Woodman [1974] QB 754 (CA)

R v Meech [1974] QB 549

R v Kelly [1999] QB 621

R v. Kelly [1998] 3 All ER 741, CA

R. v. Ghosh [1982] QB 1053

R v. Cahill [1993] Crim LR 141, CA

R v. Fernandes [1996] 1 Cr App R 175

Neal v Gribble [1978] RTR 409

Akbulut v. Grimeshaw 96 A Crim R [1991]

Akbulut v. Grimshaw [1998] 3 VR 756

International News Service v. Associated Press, 248 U.S. 215 (1918)

Chapter five

Boss Holdings v Grosvenor West End Properties [2008] UKHL 5

R v. Environment Agency [2007] UKHL 30

A v. Adamiya Investigation Court, Iraqi Court of Appeals Civil Extended Commission [2010] 289

R v. Horsman [1998] Q.B 531

R v. Smith [2002] EWCA Crim 2907

M v. K [1970] Iraqi Court of Cassation 1648

S v. H [1971] Iraqi Court of Cassation J 1697

A v. K [1971] Iraqi Court of Cassation J 177

United States v. Brown 333 U.S. 18 (68 S.Ct. 376, 92 L.Ed. 442) (1948)

R v. Goodwin [2005] EWCA Crim 3184

R v Preddy [1996] AC 815

People v. Sobiek 30 Cal. App. 3d 458 (1973)106 Cal. Rptr. 519

K and other v. Muthanna Criminal Court [2007] 173

A v. Criminal Centre Court, Iraqi Court of Cassation Five Commission [2009] 178

R v. Hinks [2001] 2 A. C. 241

United States v. Rodgers 706 F .2d 854 (8th Cir. 1983)

Black-Clawson International Ltd v Papierwerke Waldhof-Aschaffenburg AG (1975) 1 All ER 810

Magor and St. Mellons Rural District Council v Newport Corporation [1952] A.C. 189

Pepper v Hart (1992) 3 WLR 1032

Landgraf v. USI Film Prods 511 U.S. 244, 265 (1994)

Hamdan v. Rumsfeld, 126 S. Ct. 2749 (2006)

Grayned v. City of Rockford 92 S. Ct. 2294 (1972)

R v Chabers [2008] EWCA Crim. 2467

Campbell v. Bennett, 340 F. Supp. 2d 1301 (M.D. Ala. 2004)

Bynum v. State, 767 S.W.2d 769, 773 (Tex. Crim. App. 1989)

State of Texas v River Forest Development Co. 315 S.W. 3d 128 (Tex. App. Houston [1 Dist.] 2010

A and Others v. Criminal Centre Court Integrity Commission Court of Appeal Public Commission [2007] 42

M v. Criminal Central Court of Karbala Iraqi Court of Appeals Expanded

Commission [2009] 154
J and *Others v. Delinquents Court of Wasit* Iraqi Court of Cassation Extended Commission [2006] 55
S and Others v. Criminal Central Court of Baghdad Iraqi Court of Cassation Public Commission [2007] 19
Prosecutor v. Criminal Court of Basra Iraqi Court of Cassation Second Criminal Commission [2010] 2018, 2019
K and Others v. Criminal Central Court of Mesan, Iraqi Court of Cassation, Public Commission, [2010] 91
Kolender v. Lawson 461 U.S. 352, 357 (1983)
Cuevas v. Royal D'Iberville Hotel 498 So. 2d 346, 358 (Miss. 1986)
Vill. of Hoffman Estates v. Flipside Hoffman Estates Inc. 455 U.S. 489, 499 (1982)
R v. Jones and Others (2006) 2 W.L.R. 772
R v. C [2004] EWCA Crim 292
R v. Dica [2004] EWCA Crim 1103 [2004] QB 1257
Dred Scott v. Sandford, 60 U.S. 393, 19 How 393, (1857)
Pepper v Hart [1993] AC 593
United Stated v. Lyons 706 F.2d 321 (5th Cir.1984)
United States v. Neapolitan, 791 F.2d 489 (7th Cir. 1986)
Duty Prosecutor and A v. Hilla Court of Misdemeanours Federal Court of Appeal of Babylon T/J/ 30/10/2012, 455, 456
A v. Criminal Central Court of Mesan, Iraqi Court of Cassation, Criminal Commission [2006] 6178
F v. Criminal Court of Rusafa Iraqi Court of Cassation Extended Criminal Commission [2011]
United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001)
LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133-34 (9th Cir. 2009)
B&B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007)
United States v. Kozminksi 487 U.S. 931 (1988)
Catalan v. Vermillion Ranch Ltd. No. 06-CV-01043-WYD-MJW, 2007 U.S. Dist. LEXIS 567, (D. Colo. Jan. 4, 2007)
States v. Veerapol, 312 F.3d 1128, 1132 (9th Cir. 2007)
R v Clegg [1995] 2 WLR 80

R v Ireland [1998] AC 147

Fagan v Commissioner of Metropolitan Police (1969) 1QB 439

United States v. Pebworth, 112 F.3d 168, 171 (4th Cir. 1998)

United States v. Mendoza-Gonzalez, 520 F.3d 912, 915 (8th Cir. 2008)

United States v. Hurtado, 508 F.3d 603, 607 (11th Cir. 2007) cert. denied, --- U.S. ----, 128 S.Ct. 2903, 171 L.Ed.2d 843 (2008)

United States v. Montejo, 442 F.3d 213, 214 (4th Cir. 2006) cert. denied, 549 U.S. 879, 127 S.Ct. 366, 166 L.Ed.2d 138

America v. Satelo United States Court of Appeals 515 F.3d 1234, 380 U.S.App.D.C. 11

United States v. Godin 476 F. Supp. 2d 1, 2 (D. Me. 2007) U.S. 879, 127 S.Ct. 366, 166 L.Ed.2d 138 (2006)

S v. Criminal Central Court of Baghdad Iraqi Court of Appeal Public Commission [2008] 282

A v. Criminal Court of Babylon Iraqi Court of Appeals Public Commission [2007] 79

A v. Criminal Court of Diywania, Iraqi Court of Appeals, Public Commission, [2006] 158

A v. K, Court of Cassation [1971] 177

*Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000)

Ratlaf v. United States, Certiorari to the United States Court of Appeals, No. 92-1196 (9th Cir. 1994)

Ratzlaf v. United States 507 U.S. 1050, 113 S. Ct. 1942 (Mem) U.S. 1993

Morrissette v. United States, 342 U.S. 246 (72 S. Ct. 240, 96 L. Ed. 288) (1952)

United States v. Devegter, 198 F. 3d 1324, 1237-28 (11th Cir. 1999)

United States v. Woodard, 459 F. 3d 1078, 1086 (11th Cir. 2006)

United States v. Lemire, 720 F.2d 1327, 1336 (D.C Cir. 1983)

United States v. Bohonus, 628 F.2d 1167, 1172 (9th Cir.) cert. denied, 447 U.S. 928, 1000 S. Ct. 3026, 65 L. Ed. 2d 1127 (1980)

United States v. Reece, 614 F. 2d 1259, 1261 (10th Cir. 1980)

United States v. Bryza, 522 F. 2d 414, 422 (7th Cir. 1975), Cert. denied, 426 U.S. 912, 96 S. Ct. 2237, 48 L. Ed. 2d 414, 422 (7th Cir. 1975)

H v CPS [2010] EWHC 1374 (Admin) Division Court

Reginal v Unah [2011] EWCA Crim 1837

United States v. Condolen, 600 F. 2d 7, 8 (7th Cir. 1979)

United States v. Louderman, 576 F. 2d 1383, 1387-88 (9th Cir.), Cert. denied, 439 U.S. 896 S. Ct. 257, 58 L. Ed. 2d 243 (1978)

A v. K, Federal Court of Appeal of Babylon T/J/ 2012, 26/9/2012, 363

Regina v Jones and *Others* (2006) 2 WLR 772

S v. H [1971] Court of Cassation 1697

G v. D [1970] Court of Cassation 286

Chapter six

Yam v. R [2010] EWCA Crim 2072

Darwin & Anor, R. v R [2009] EWCA Crim 860

Sammon v R [2011] EWCA Crim 1199

Sofroniou v. R [2003] EWCA Crim 3681

Gobbons and others v. R [2002] EWCA Crim 3161, [2003] 2 Cr App Rep (S) 34, [2003] Crim LR 419, [2003] 2 Cr App R (S) 34

Sward v R [2005] EWCA Crim 1941

Olden, R. v R [2007] EWCA Crim 726

R. v Ayodele Odewale and Other [2004] EWCA Crim

R v Williams [2009] EWCA Crim 2194

Pigott v R [2009] EWCA Crim 2292, [2010] 2 Cr App Rep (S) 16, [2010] 2 Cr App R (S) 16, [2010] Crim LR 153, [2010] Lloyd's Rep FC 97

King v. DPP [2008] EWHC 447 (Admin)

R v. William [1980] Crim LR 589

R v.Lambie [1982] AC 449

Ellis v DPP {[2001] EWHC Admin

R v Cropp 05/07/1991[1991] 7 CLSR 168, [1991] CL&P; [1992] 3 WLR 432

R v Bignell 1997, [1998] 1 Cr. App. R. 1

R v Raphael Gray, Swansea Crown Court 2001

DPP v Lennon [2006] EWHC 1201

R. v Bow Street Magistrates' Court Ex p. Allison [2000] 2 A.C. 216

McKinnon, R v. Secretary of State for Home Affair [2009] EWHC 2021 (Admin)

Zezev and Yarimaka v. the Governor of HM Prison Brixton and the Government of the United States of America [2002] EWHCA 589 (Admin)

United States v. Godin, 534 F.3d 51 (1st Cir. 2008)

United States v. Hill (E.D. Va. May 17, 2004)

United State of America v. Ozuna-Carbrera, 663 F 3d (1st Cir. 2011)

United Sates v. Lumbard, 706 F.3d 716 C. A. 6 (Mich.) 2013

U. S. v. Hilton, 701 F.3d 959 C.A. 4 (N. C) 2012

United States v. LaFaive, 618 F.3d (7th Cir. 2010)

United States v. Maciel –Alcala 612 F.3d (9th Cir. 2010)

U.S. v. *Zuniga-Arteaga*, 681 F.3d 1220 C.A 11 (Fla.) 2012

Flores-Figueroa v. U.S., 556 U.S. 646, 129 S. Ct. 1886 (2009)

United States of America v. Gaspar, 344 Fed. Appx. 541(11th Cir. 2009

U.S. v. Grajeda Gutierrez, 372 Fed. Appx. 890(10th Cir. 2010)

United States v. Holmes, 595 F.3d 1255 (11th Cir. 2010)

United States v. Ronald D. Adkins, 372 Fed. Appx. (6th Cir. 2010)

United States v. Gomez-Castro, 605 F.3d 1245 (11th Cir. May 13, 2010)

United States v. Gomez, 580 F.3d 1229 (11th Cir. 2009)

U.S. v. Novas, 461 Fed. Appx.896 (11th Cir. 2012)

United States v. Villanueva-Sotelo, 515 F.3d 1234, 380 U.S. App. D.C. 11 2008

Kansas v. Bradly D. Hardesty, 42 Kan.App.2d 431, 213 P.3d 745 Kan. App. [2009]

United State of America v. Ozuna-Carbrera, 663 F 3d 496 (1st Cir. 2011)

United States v. Retana, 641F. 3d 272, 273-75 (8th Cir.2011)

United States v. Mobley, 618 F.3d 539, 547-48 (6th Cir.2010)

United States v. Abdelshafi 592 F.3d 602 (4th Cir. 2010)

Table of Statutes

1968 Theft Act c. 60 (UK)

Criminal Law 1967 c, 58 (UK)

Model Penal Code 1962 R 12. 9. 5 (US)

Iraqi Penal Code 111of 1969

Criminal Code R.S.C.1970, c. C-34 (Canada)

Identity Theft and Assumption Deterrence Act 1998 (a) (7) Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998)

United States Sentencing Guidelines § 2b1.1 (12), 2001

Identity Theft Penalty Enhancement Act 2004 Public Law 108-275, 118 Stat. 831(Jul. 15, 2004)

Mail Fraud and Other Fraud Offences 18 U.S. Code Ch.63 Pub. L. 113-65

Data Protection Act of 1998 (Commencement No. 3) Order 2011 N0. 601 (c. 21) (UK)

Fraud Act 2006 c. 35 (UK)

Computer Misuse Act 1990 c. 18 (UK)

Criminal Attempt Act 1981 c. 47 (UK)

Iraqi Constitution 1970

Iraqi Information Crimes Project 2011

Fair Credit Report Act of 1970, S 3, available at <http://www.ftc.gov/os/statutes/031224fcra.pdf> accessed on 22 May 2011

CBA, Bill S-4, An Act to Amend the Criminal Code (Identity Theft and Related Misconduct), 2009 available at <http://www.cba.ca/contents/files/submissions/sub_20090603_01_en.pdf> accessed on 25 May 2011

Fair and Accurate Credit Transactions (FACT) Act of 2003 (FACT Act), Pub. L. No. 108-159, 117 Stat. 1952 (Dec. 4, 2003)

South Australia Criminal Law Consolidate Act of 1935 s 144C amended in 2003

Queensland Criminal Act of 1899 s 408D ins 2007 No. 14 s16 and amended in 2010, s 1 (4)

Victoria's Crimes Amendment Act 2009, section 192B No.22 of 2009

Western Wales Criminal Code Amendment (Identity Crime) Act 2010, (No. 16 of 2010)

South Wales's Crimes Amendment (Fraud, Identity and Forgery Offences) Bill 2009

Iraqi Penal Act No. 111 of 1969

Accessories and Abettors Act 1861 c. 94 (Regnal. 24_and_25Vict)

Libyan Penal Code 1953

Egypt institutional, No. 3 1937

Syrian Penal Code No. 148, 1949

US Model Penal Code (1985)

Iraqi Constitution 1970

Egyptian Penal Code 1937

New York Penal Law (McKinney 2009)

The Saudi Arabia Electronic Information Crimes Law No. 79 of 2007 (4)

Sudan Information Crimes Law of 2007

Combating Information Technological Crimes Law of United Arab Emirates 2006

Information Technological Crimes Law of United Arab Emirates No. 5 of 2012

Reports

SKM, 'Judges of Basra Request Enacting Legislation to Curb Electronic Crime and they warn from using it within the Scope of Organized Crime' ALMada Press available at <http://www.almadapress.com/ar/news/11496/> accessed on 21 June 2013

The President's Identity Theft Task Force, Combating Identity Theft a Strategic Plan' April 2007 available at <http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/downloadabledocuments/combating_identity_theft_a_strategic_plan.pdf> viewed on 17 February 2011

National Fraud Authority, 'Identity Theft Costs UK £2.7 Billion Every Year' 2010 available at <http://www.attorneygeneral.gov.uk/nfa/whatarewesaying/newsrelease/pages/identity-fraud-costs-27billion.aspx> viewed on 2 May 2011

Aswat Al- Iraq News June 25, 2012 available at <http://ar.aswataliraq.info/%28S%28exmpmvvvgvvbgn555gbtzu45%29%29/Default1.aspx?page=article_page&id=300354> accessed on 19 June 2013

Iraqna Ikhbariya Shabaka, June 25, 2012 available at <http://translate.google.com/#en/ar/Ikhbariya> accessed on 19 June 2013

Bureau of Justice Statistics, 2006, 'Identity Theft' 2004, Washington, DC: U.S. Government Printing Office

The Bureau of Justice Statistics report, 2006

Better Business Bureau, 'New Research Shows That Identity Theft is More Prevalent Offline Than Online, Press' January 26, 2005 available at <http://www.bbb.org/us/article/new-research-shows-that-identity-theft-is-more-prevalent-offline-with-paper-than-online-519> accessed on 6 July 2011

Cabinet Office, 'Identity Fraud: A Study' 2002 available at <http://www.statewatch.org/news/2004/may/id-fraud-report.pdf> accessed on 19 July 2011

United Kingdom Home Office (2006a), 'Identity Crime Definitions' available at <http://www.identity-theft.org.uk/definition.html> accessed on 16 February 2011

Identity Theft Resource Centre, 'Identity Theft: The Aftermath 2003

A Comprehensive Study to Understand the Impact of Identity Theft on Known Victims' available at <http://www.idtheftcenter.org/artman2/uploads/1/The_Aftermath_2003.pdf> accessed on 22 May 2011

U.S. Department of Justice, <http://www.usdoj.gov/usao/mt/identity_theft/> accessed on 20 May 20011

English Commission Law no. 186, Paragraph 2.11-2.15, 11-12

Press Release, 'LixesNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access' April 12, 2005 available at: <www.lixesnexis.com./about/releases/0789.asp.> accessed on 12 August 2011

Press Release, 'New Leahy Bill Targets "Phishing" and "Pharming"' Senator Patrick Leahy, Speech on the Senate Floor on the Introduction of the 'Anti-Phishing Act of 2005' (Feb. 28, 2005) [hereinafter Leahy Speech] available at <http://www.senate.gov/galleries/daily/224pr05.html#anchor334628> accessed on 12 July 2012

'According to Report Published in February 2006 by UK Home Office' available at <http://www.identitytheft.org.uk/cms/assets/Cost_of_Identity_Fraud_to_the_UK_Economy_2006-07.pdf> accessed on 9 May 2011

U.S. Department of Justice, 'Identity Theft, Problem-Oriented Guides for Police, Problem-Specific Guides Series' No. 25 (June 2004) available at <http://www.cops.usdoj.gov/mime/open.pdf?Item=1271 > accessed on 27 May 2011

U.S. Department of Justice, National Institute of Justice, 'Identity Theft-A Research Review' 2007, available at <https://www.ncjrs.gov/pdffiles1/nij/218778.pdf> access on 7 May 2011

U.S. General Account Office, 'Identity theft: Greater Awareness and Use of Existing Data are Needed. Report to the Honorable Sam Johnson, House of Representative'

2002a, 62. Washington, D.C. [G A O-02-766] available at <http://www.consumer.gov/idtheft/reports/gao-do2766.pdf> accessed on 20 December 2011

DPS, Law Enforcement Academy, Santa Fe, New Mexico, 'Criminal Law: White Collar Crimes Online' "without year" available at <http://www.dps.nm.org/trainig/legal/documents/White_Collar_Crime.pdf> accessed on 21 May 2011

OECD, 'Organization for Economic Co-operation and Development, OECD Policy Guidance on Online Identity Theft' 2008 available at <http://www.oecd.org/dataoecd/49/39/40879136.pdf> accessed on 5 July 2011

Florida, Sixteenth State-wide Grand Jury (Jan. 10, 2002), 'State-wide Grand Jury Report: Identity theft in Florida First Report of Sixteenth Stat- wide Grand Jury' available at <http://myfloridalegal.com/pages.nsf/4492d797dc0bd92f85256cb80055fb97/758eb848bc624a0385256cca0059f9dd!OpenDocument> accessed on 10 May 2011

ISPAC, 'The Evolving Challenge of identity-Related Crime: Addressing Fraud and the Criminal Misuse and Falsification of Identity' Edited by D Chryssike, N Passas and Ch D Ram, 2008 available at <http://www.ispac-italy.org/pubs/ISPAC%20-%20Identity%20Theft.pdf> accessed on 6 July 2011

Synovate, Federal Trade Commission – 'Identity Theft Survey Report' 2003 available at <http://www.ftc.gov/os/2003/09/synovatereport.pdf> accessed on 11 May 2

Identity Theft 911, 'Exploiting the Dead, Identity Theft 911' New Sletter Vol.7 (2) February, (2010) available at <http://idt911.com/en/KnowledgeCenter/~/media/537D837CD5A44EF1A50AA7C818EB5251.ashx> accessed on 25 May 2011

Canadian Internet Policy and Public Interest Clinic (CIPPIC), 'Identity theft: Introduction and Background' CIPPIC Working Paper No.1 (Identity Theft Series) 2007 available at <http://www.cippic.ca/documents/bulletins/Introduction.pdf> accessed on 1 July 2011

BBC News, 'Who, What, Why: Is Taking Rubbish Illegal?' 31 May 2011, available at <http://www.bbc.co.uk/news/magazine-13037808> accessed on 12 May 2014

PRC, Cases from PRC Hotline, 'Privacy Rights Clearinghouse' (PRC 2004-2006) available at <http://www.privacyrights.org/cases/cases2004-2005.htm> accessed on 31 October 2010

Federal Trade Commission, 'Take Charge Fighting Back against Identity Theft' (Report) (2004) available at <http://www.talgov.com/tpd/pdf/tc-fbaidt0605.pdf> accessed on 20 December 2011

Federal Trade Commission, 'Take Charge Fighting Back against Identity Theft' (report), (2005) available at <http://www.wcso.net/data/TakeCharge.pdf> accessed on 2 August 2011

Idtheft,

911.com,http://wwwidentitytheft911.com/education/articles/art20040915guilty.htm

Federal Trade Commission (2000), 'Identity Theft Victim Complaint Data: Figures and Trends on Identity Theft' January 2000 through December 2000, available at <http://www.ftc.gov/bcp/workshops/idtheft/chart-update.pdf> accessed on January 22, 2014

Team of Hiregange- Bangalore and Hyderabad, 'What is the Service Tax, Service Tax Concepts Updated Upto 01. 10. 2012' available at <www.simpletaxindia.net> accessed on 22 January 2014

Techniques of Identity Theft, CIPPIC Working Paper No. 2 (ID Theft Series) 2007 available at <https://www.cippic.ca/sites/default/files/IDT_No.2-Techniques.pdf > accessed on 9 May 2014

Business Wire, 'LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access; Company Takes Steps to Notify Consumers and Provide Monitoring and Support to Prevent Identity Theft' April 12 2005, available at: <http://www.allbusiness.com/crime-law-enforcement-corrections/criminal-offenses-fraud/5076522-1.html> accessed on 2 August 2011

New York Times, July 22, 2003, Technology Briefing, 'Internet: F. T.C. Settled Suit Against Youth in Net Fraud' available at <http://www.nytimes.com/2003/07/22/business/technology-briefing-internet-ftc-settles-suit-against-youth-in-net-fraud.html> accessed on 3 August 2011

Berkeley 'Theft Exposes Data of 100,000' AP Associated Press (28 March, 2005) available at <http://www.msnbc.msn.com/id/7320552/ns/technology_and_science-security/t/berkeley-theft-exposes-data/> accessed on 30 Oct. 2010

Testimony, at <http://judiciary.senate.gov/testimony.cfm?id/=1437&_i729> in S Sproule and N Archer, 'Defining Identity Theft – A Discussing Paper' McMaster eBusiness Research Centre McMaster University 2006 available at <http://www.business.mcmaster.ca/idtdefinition/IDT%20Discussion%20Paper%20Revision%20from%20Sue%20Sproule%20April%206%2006.pdf> accessed on 10 August 2011

Federal Trade Commission (2000b), 'Identity Theft Victim Complaint Data: Figures and Trends on Identity Theft. Retrieved 20 November 2000' available at <http://www.ftc.gov/bcp/workshops/idtheft/chart-update.pdf> accessed on 15 November 2010

U.S. General Account Office (GAO 2002a June), 'Identity Theft: General Awareness and Use of Existing Data Need. Report to the Honorable Sam Johnson, House of Representative Washington, D.C. [G A O-02-766]' available at <http://www.consumer.gov/idtheft/reports/gao-d02766.pdf> accessed on 17 Jan. 2014

The Law Commission, Law Com No 305, 'Participation in Crime, Presented to the Parliament of the United Kingdom by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty' 2007 available at <http://lawcommission.justice.gov.uk/docs/lc305_Participating_in_Crime_report.pdf> accessed on 20 December 2011

Iraqi Civil Society News, January 6, 2013 available at <http://www.almubadarairaq.org/?p=349> accessed on January 12, 2014

Attorney General's Reference (No. 140 of 2004) [2004] EWCA Crim 3525

Memorandum from the Society for Computers and Law—Internet Interest Group and Privacy and Data Protection Interest Group paragraph 5 available at <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/7012402.htm> viewed on 25 March 2012

All Party Internet Group, '"Revisions of the Computer Misuse Act': Report of an Inquiry by the All Party Internet Group' 2004 available at

<http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry/CMAReportFinalVersion1.pdf> accessed on 3 October 2011

Web Resources

Al- Qaysiyah A, 'Crimes Dividing According to the *Actus Reus*' available at <http://www.lawjo.net/vb/showthread.php?t=11879> viewed on 28 August 2011

Allison S F. H., 'Case Study of Identity Theft' 2003 available at <http://etd.fcla.edu/SF/SFE0000093/MasterThesis.pdf> 22 accessed on 5 March 2011

Al-Hakim N, 'Electronic Crimes Cost Saudi Arabia Billion Rial' Okaz Newspaper, 27 January 2012 available at <http://www.okaz.com.sa//Issues/20120127/Con20120127473133.htm> viewed on 24 Mar. 2013

Al-Darraji A, 'With the Increasing of Invitation to Enact the Project of Information Crimes in Iraq' 6th of December 2012 Muwatin Newspaper, available at <http://www.almowatennews.com/news.php?action=view&id=43770> viewed on 24 March 2013

Al-Isawi K, 'UNESCO Iraq Branch Held a Conference to Discuss Information Crime Project' Al-Marsad News, available at <http://www.almarsadnews.org/security-and-policity/6319.html> accessed on 21 Jun 2013

Abood Z, 'an Opinion in Draft of Information Crimes Project of 2011' Judicial Magazine 3/12/2012 available at <http://www.iraqja.iq/view.1705/> accessed on 13 March 2013

Anderson K B, 'Identity Theft: Does the Risk Vary With Demographics?' (2005) available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=795427> accessed on 27 May 2011

Adams 'The Identity Theft Project Report' and Assumption Deterrence Act of 1998: How Effective Is It in Combating Identity Theft' 15 December 2001 available at <http://gsulaw.gsu.edu./lawand /papers/fa00/adams > accessed on 26 May 2011

Aguero N, Gandy B, Laoang R, Mejia J, Vandlez B, MIS 304 and Fang F, 'Cybercrimes and Countermeasures' 2010 available at <http://public.csusm.edu/fangfang/Teaching/HTMmaterial/StudentProjectSpring2010/Group7Paper.pdf > accessed on 15 November 2010

Atallah S, 'The Actus Reus of Theft' 2011 available at <http://www.shaimaaatalla.com/vb/showthread.php?t=9963> accessed on 9 March 2013

Al Musawi S, 'The Analogy in Criminal Law (comment on the decision of Federal Court of Appeal of Babylon as Court of Cassation)' Modern Argument No. 3907, 10/11/2012 available at <http://www.ahewar.org/debat/show.art.asp?aid=331863> accessed on 10 March 2013

Al Musawi S, 'The Definition of Terrorist Crime', Shabaka Al Nabaa News 29/11/2008, available at <http://www.annabaa.org/nbanews/72/067.htm> accessed on 12 March 2013

Al Zarqani T, 'The Iraqi Parliament Abolishes the Information Crimes Project Due to not Need It and Iraqis Have Rejected, Agad Neze Wekala for News, It' 5th of February 2013 available at <http://www.akadnews.org/مجلس-النواب-يلغي-قانون-جرائم-المعلوم/> accessed on 12 January 2014

Behar R, 'In Information Crimes, It Is Necessary to Prepare Security and Judicial Measures for Searching, Investigation, and Trial' Justice News 5 February 2013 available at <http://thejusticenews.com/?p=9679> accessed on 23 Mar. 2013

Bhari R, 'In Crimes of Information It Is Necessary to Provide Security and Judicial Measures in Search, Investigation and Trial, the Modern Crimes Constitute Challenge to the Iraqi Security 2013, 5/2/2013 available at <http://thejusticenews.com/?p=9679> accessed on 15 March 2013

Baum K, 'Identity Theft' (2004) Bureau of Justice Statistics Bulletin 2006 U.S. Department of Justice Office of Justice Programs, available at <http://www.bjs.gov/content/pub/pdf/it04.pdf > accessed on 20 June 2013

Benner J, et al, 'Nowhere to Turn: Victims Speak Out on Identity Theft ACalpirg/ PRC Report' 2000 available at <http://www.popcenter.org/problems/credit_card_fraud/PDFs/identity%20CALPYRG.pdf > accessed on 22 May 2011

Bell L, 'Offline Identity Theft-Not All Theft Happens Online' 2007 available at <http://ezinearticles.com/?Offline-Identity-Theft---Not-All-Identity-Theft-Happens-Online&id=5862168> accessed on 6 July 2011

Borrus A, 'To Catch an Identity Thief' Business Week, (March 31, 2003) available at <http://www.busniessweek.com/magazine/content/03/b3826071_mz020.htm> accessed on 25 May 2011

Bonneau P J and Hajeski J W, 'Identity Theft- Is it a Cryptographic Problem?' an Interactive Qualifying project Report Submitted to the Faculty of the Worcester Polytechnic Institute, March 14, 2005 available at <http://www.crypto.wpi.edu/publictions/Documents/WPI_IOP_IdTheft.pdf,> accessed on 27 September 2010

Bhasin M, 'Mitigating Cyber Threats to Banking Industry, Information Technology' 2007available at <http://www.icai.org/resource_file/96551618-1624.pdf,> accessed on 27-Oct-2010

Cavoulcian A, 'Identity Theft: Who's Using Your Name? Information and Privacy Commissioner/ Ontario' 1997 available at <http://www.ontla.on.ca/library/repository/mon/10000/197561.pdf> accessed on 2 June 2011

Cherry S R, 'Al-Qaeda May Be Stealing Your ID, Insight on the News' Aug. 26, 2002 available at <http://findarticles.com/p/articles/mi_m1571/is_31_18/ai_90990420/pg_2/?tag=mantle_skin;content> accessed on 25 May 2011

Cheney J S, 'Identity Theft: Do Definitions Still Matter?' (2005) Discussion Paper Payment Credit Card Centre 11 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=815684> accessed on 2 February 2014

Chen T M, Elder M C, and Thompson J, 'Handbook, Chapter 74, Electronic Attack' 2005 available at <http://lyle.smu.edu/~tchen/papers/handbook2005.pdf> accessed on 14 November 2010

Chik Warren B., 'Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore' 2007 available at<www.**law**.ed.ac.**uk**/ahrc/comp**law**/docs/**chik**.doc> accessed on 15 July 2012

Copes H and Veraitis L, 'Identity Theft' (2009) available at <http://www.uk.sagepub.com/haganintrocrim7e/study/features/articles/HB14.1.pdf> accessed on 23 Jun. 2011

Copes H and Veraitis L, 'Identity Theft: Assessing Offenders' Strategies and Perception of Risk' Technical Report for the National Institute, NCJRS219122, NIJ Grant No.2005-IJ-CX-0012. 2007 available at <http://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf> accessed on 9 May 2011

Dickson C J, Beat E, L M Wilson, and JJ Le Dain, Indexed as *R. v. Stewart*, File No. : 17827, 26 May [1988] 1 S.C.R. 963 available at <http://scc.lexum.org/en/1988/1988scr1-963/1988scr1-963.html> accessed on 10 December 2011

Elston M J and Stein A S, 'International Cooperation in Online Identity Theft Investigation: Hopeful Future but a Frustrating Present. Computer Crime and Intellectual Property' (without year) Section, United States department of justice P.O. Box 887, Frank Station Washington D.C. 20044-0887, 2002 available at <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf > accessed on 10 August 2011

Evans B, 'Computer: Hacker How Best to Solve It', 15 July 2008 lawdit readingroom available at <http://www.lawdit.co.uk/reading_room/room/view_article.asp?name=../articles/5167-Computer-Hacking-How-Best-To-Solve-It.ht> viewed on 2 October 2011

Finklea Kristen M, 'Identity Theft: Trends and Issues, CRS Report for Congress' 2012 available at <http://www.fas.org/sgp/crs/misc/R40599.pdf> accessed on 23 May 2013

Emigh A and Labs R, 'Online Identity Theft: Phishing Technology Chokepoints and Countermeasures' 2005 available at <http://www.antiphishing.org/Phishing-dhs-report.pdf> accessed on 5 July 2011

Fearon D James, 'What is Identity (as We Now Use the Word)' (1999) available at <http://www.stanford.edu/~jfearon/papers/iden1v2.pdf> viewed on 30 March 2012

Farrow R, 'Source Address Spoofing: Forged Address Aid Internet Attaches, Here's what to do about them' 2 November 2010 Network Magazine available at <http://technet.microsoft.com/en-us/library/cc723706.aspx> accessed on 23 November 2010

Flaming T H, 'The National Stolen Property Act and Computer Files: A New Form of Property, a New Form of Theft' 1993 The University of Chicago Law School Roundtable available at <http://heinonline.org/HOL/Page?handle=hein.journals/ucroun1993&div=15&g_sent=1&collection=journals> viewed on 29 December 2011

Freedman CD, 'The Extension of the Criminal Law to Protecting Confidential Commercial Information: Comments on the Issues and the Cyber-Context' 2005 available at <http://www.bileta.ac.uk/99papers/freedman.html> viewed on 27 June 2011

Fafinski S and Misassian N, 'UK Cybercrime Report 2009' 2009 available at <http://zunia.org/uploads/media/knowledge/613-GRLK_PRD1256978512.pdf> viewed on 10 March 2012

Green S P, 'Theft by Omission' 2009 Rutgers School of Law- Newark, Research Report No. 050 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1410855> viewed on 12 February 2012

Geddes RS, 'Purpose and Context in Statutory Interpretation' available at <http://www.judcom.nsw.gov.au/publications/education-monographs-1/monograph4/07_geddes.pdf> viewed on 10 January 2012

Gayer J, 'Policing Privacy: Law Enforcement's Response to Identity Theft' California CALPRIG Education Fund 2003, 13 available at <http://calpirgorg.stage.pubintnet-dev.org/sites/pirg/files/reports/policingprivacy2003.pdf> accessed on 20 May 20011

Gerard G J and Hillison W and Pacini C., 'Identity Theft: An Organization's Responsibilities' 2004 available at <http://ruby.fgcu.edu/courses/cpacini/courses/common/idtheftjoffincrim.pdf> accessed on 31 Oct. 2010

Graham B, 'The Evolution of Electronic Payments, School of Technology' and Electrical Engineering, the University of Queensland, October 2003 available at <http://innovexpo.itee.uq.edu.au/2003/exhibits/s334853/thesis.pdf> accessed on 3 October 2010

Gallant K S, 'The Principle of Legality in International and Comparative Criminal Law' (2007) available at

<http://www.gistprobono.org/sitebuildercontent/sitebuilderfiles/internationalcomparativecriminallaw306.pdf> accessed 22 April 2011

Haddad W, 'If You Wants to Be a Unique Lawyer You Should Know These Crimes' 2008 available at <http://pbapls.3arabiyate.net/t41-topic> viewed on 27 August 2011

Hoar B, 'Identity theft: The Crime of the New Millennium' USA Bulletin, (March, 2001) Vol. 49 (2) U S Department of Justice available at <http://www.justice.gov/criminal/cybercrime/usamarch2001_3.htm> accessed on 17 Feb. 11

Hughes K, 'Final Report of Cognitive Research on the New Identity Questions for the 2004 National Crime Victimization Survey, Studies Series' (Survey, Methodology =2004-02) 15. Washington, D.C.: Statistical Research Division, U.S. Bureau of the Census Washington D.C. 20233 Available at <http://www,cesus.gov/srd/parpers/pdf/ssm2004-02.pdf> accessed on 26 May 2011

Hoofnagle C J, 'Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors' (2005) Stanford University Press 5 available at <http://papers.ssrn.co/sol3/papers.cfm?abstract_id=650162> accessed on 27 May 2011

Hoffman S K and McGinley T G, 'Identity Theft' (2010) available at <http://legalchoice.net/freedocs/IDTR.pdf> viewed on 1 May 2011

Hoofnagle C J, 'Internalizing Identity Theft' 2010 University of California Journal of Law available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1585564> accessed on 27 May 2011

Hoor B, 'Identity theft: The Crime of the New Millennium' USA Bulletin US department of Justice, March 2001 available at <http://www.justice.gov/criminal/cybercrime/usamarch2001_3.htm> accessed on 23 May 2011

Halligan R M, 'Duty to Identify, Protect Trade Secrets Has Risen' (2005) The National Law Journal, the Weekly Newspaper for Local Profession, available at <http://www.thetso.com/Info/National%20Law%20Journal%20Article.pdf> viewed on 30 December 2011

Clayton H, 'Hole-in-the-Wallet Machine' 2003 Financial Times (London) in D B Owen, 'The State of Malware' (without year) 10 available at

<http://danielowen.com/files/The_Stae_of_Malware.pdf > accessed on 3 November 2010

Jamieson R and Stephen G, 'An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organization Impacts' 2007 available at <http://www.pacis-net.org/file/2007/1271.pdf> accessed on 28 May 2011

Janczewski L J and Colarik A M, 'Cyber Warfare and Cyber Terrorism, Information Science Reference' 2008 available at <http://www.sclindow.net/MM/CyberWarfareandCyberTerrorism.pdf> accessed on 10 November 2010

Johnson M and Rogers K M, 'The Fraud Act 2006: The E-Crime Prosecutor's Champion or the Creator of a New Inchoate Offence?' 2007 available at <http://www.bileta.ac.uk/content/files/conference%20papers/2007/The%20Fraud%20Act%202006%20-%20The%20E-Crime%20Prosecutor%27s%20Champion%20or%20the%20creator%20of%20a%20new%20inchoate%20offence.pdf> accessed on 12 January 2014

Kshirsagar P, 'The Problem of Identity Protection in Cyberspace and Some Suggestions' available at <http://ssrn.com/abstract=1520204> viewed on 27 May 2012

Kelly John X, 'Computer Misuse Essential' 1 February 2007, available at <http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseEssentials.aspx> accessed on 3 October 2011

Linda and J Foley Exec. 'Directors, Identity Theft Aftermath 2003 (Identity Theft Resource Center, A Comprehensive Study – to Understand the Impact of Identity Theft on Known Victims as well as Recommendations for Reform 2003)' available at <http://www.idtheftcenter.org/vg120.shtml> accessed on 17 March 2011

Lyzhina S and Zaghid Y., (trs), 'The Unsolved Riddle of Princess Anastasia, Pravda (Russia)' (13 July 2004) available at <http://english.pravda.ru/history/13-07-2004/6156-nicholas-2/ > viewed on 4 May 2011

Loibl T R, 'Identity Theft, Spyware and the Law' (2005) Kennesaw State University available at <http://delivery.acm.org/10.1145/1110000/1107650/p118-loibl.pdf?ip=147.143.87.65&CFID=33869448&CFTOKEN=23035291&__acm__=1312286154_530c57fbd5c8cc54ebff6a8228314c9b> accessed on 4 November 2010

Levinson C, 'Hackers Attack Iraq Vulnerable to Cybercrime' USA Today, 29 August 2008 available at <http://usatoday30.usatoday.com/tech/news/computersecurity/hacking/2008-08-28-iraqhackers_N.htm?csp=tech> accessed on 30 May 2013

Lyzhina S, and Zaghid Y, Trans, 'The Unsolved Riddle of Princess Anastasia, Pravda (Russia)' (13 July 2004) available at <http://english.pravda.ru/history/13-7-2004/6156-nicholas-0/> viewed on 4 May 2011

Meulen N, 'The Challenge of Countering Identity Theft: Recent Developments in the U.S., the U.K and the E.U' International Victimology Institute Tilburg. September (2006) available at <http://www.samentegencybercrime.nl/UserFiles/File/Rapport%20identiteitsfraude%20universiteit%20tilburg.pdf> accessed on 25 May 2011

Meulen N and Koops B J, 'The Challenge of Identity Theft in Multi-level Governance Towards a Co-Ordinated Action Plan for Protection and Empowering Victims' 2009 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1447324> accessed on 27 May 2011

Morgan C A, 'Minimizing Identity Theft: Fact, Fiction, or Futile, Bowie State University Maryland in Europe' April 2oo7 available at <http://faculty.ed.umuc.edu/~sdean/ProfPaps/Bowie/T3-0607/Morgan-C.pdf> accessed on 5-Oct-2010

Newman G and McNally M, 'Identity Theft Literature Review' 2005 available at <http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf> accessed on 10 August 2011

Lee Hyunggak, 'Property in Criminal Law' Dissertation of Yonsei University (1988)

McGowan D, 'The Trespass Trouble and The Metaphor Muddle' (2004) Legal Studies Research Paper Series Research Paper No. 04.5 available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=521982> viewed on 20 November 2011

Mokhtar A, 'Nullum Crimen, Nulla Poena Sine Lege: Aspects and Prospects' 2005 available at <http://slr.oxfordjournals.org/content/26/1/41.full.pdf> accessed on 13 August 2011

MacEwan N, 'The Computer Misuse Act 1990: Lessons from its Past and Prediction to Its Future' (2008) Vol. 12 Criminal Law Review

McCullagh D, 'Season Over 'Phishing'?' CNET News com, July 15, (2000) available at <http://zdnet.com/2100-1105_2-5270077.htm1> accessed on 2 February 2011

Owen D B, 'The State of Malware' (without year) available at <http://danielowen.com/files/The_State_of_Malware.pdf> viewed on 3 November 2010

Phue C, Lee V, Smith K and Gayler R, 'A Comprehensive Survey of Data Mining-based Fraud Detection Research' 2005 available at <http://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf > accessed on 28 May 2011

O'Brien T L., 'Identity Theft Is Epidemic, Can Be Stopped' New York, Times (2004 4October) section 3:1 available at <http://www.nytimes.com/2004/10/24/business/yourmoney/24theft.html> accessed on 21 Feb. 11

Ohlin J D, 'Joint Intentions to Commit International Crimes' (2010) available at <http://www.law.upenn.edu/academics/institutes/ilp/2010papers/OhlinJointIntentionsInternationalCrimes.pdf> accessed on 6 July 2011

Paget F, 'Identity Theft' MacAfee Avert Labs, White Paper l, 2007 available at <http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf> accessed on 15 November 2010

Qaisi A, 'Crimes Dividing According to the *Actus Reus*' available at <http://www.lawjo.net/vb/showthread.php?t=11879> viewed on 28 August 2011

Robison N, Graux H, Prrilli D M, Klautzer A and Valeri L, 'Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report' 2011, 15 available at <http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf> accessed on 24 Jun. 2013

Ronderos J G 'Identity Fraud and Transnational Crime' Paper Presented to the Meeting of the CSCAP Working Group on Transnational Crime, Manila Philippines, May 31June 2000 available at <http://www.ncjrs.gov/nathanson/id_fraud.html> accessed on 26 May 2011

Rusch J J, 'Making a Federal Case of Identity Theft: the Department of Justice's Role in the Theft Enforcement and Prevention' 2000 available at <http://www.usdoj.gov/criminal/fruad/fedcase_idtheft.html> on 8 February 2012 in

Newman G R, McNally M M, 'Identity Theft Literature Review' (2005) available at <https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf > accessed on 10 August 2011

Ryan P and Habirson A, 'The Law on Computer Fraud in Ireland-Development of the Law and Dishonesty' (2009) available at <http://www.arthurcox.com/uploadedFiles/Publications/Publication_List/Arthur%20Cox%20-%20The%20Law%20on%20Computer%20Fraud%20in%20Ireland,%20June%202010.pdf> viewed on 8 February 2012

Ramasastry A, 'The Anti-Phishing Act of 2004: A Useful Tool Against Identity Theft' 2004 available at <http://writ.news.findlaw.com/ramasastry/20040816.html> accessed on 22 March 2012

Robinson James K, 'Remarks at the International Computer Crime Conference: Internet as the Scene of Crime' (2000) available at <http://www.usdoi.gov/criminal/cybercrime/roboslo.htm> viewed on 8 April 2012

Saleh W, 'Hacking in Iraq: Extortion and Destroyed Government Websites' Elaf Newspaper, February 24, 2012 available at <http://www.elaph.com/Web/Technology/2012/2/718471.htm> accessed on 2 June 2013

Seljan S et al, 'E-Identity: Responsibility or Commodity' 2007 available at <http://infoz.ffzg.hr/INFuture/2007/pdf/3-05%20Seljan,%20Stancic,%20Crnec,%20Salopek,%20E-identity.pdf> accessed on 6 July 2011

Steven L and Altholz N, 'Rootkits for Dummies 'Chapter 1, Much Ado about Malware' 2007 available at <http://www.sec88.com/book/Sec/RootKits_FD.pdf> accessed on 10 October 2010

Spurlock K and Wyatt D, 'The Internet Security Dilemma' California State University 17 May 2007 available at <http://public.csusm.edu/fangfang/Teaching/HTMmaterial/StudentprojectSlides-Sprg2007/FinalPaper-1-5.pdf> accessed on 15 October 2010

Sipior J C, Ward T, and Rosell R, 'A United States Perspective on the Ethical and Legal Issues of Spyware' (2005) available at <http://cs.potsdam.edu/faculty/laddbc/Teaching/Ethics/StudentPapers/2005ipior-

AUnitedStatesPerspectiveOnTheEthicalAndLegalIssuesOfSpyware.pdf> accessed on 2 August 2011

Salhuana M and Groves L, 'Investigation of Security Breaches of Popular Web Browsers' 2005 available at <http://enpub.fulton.asu.edu/iacdev/courses/CSE494-598IA/Fall2005/files/projects/Final_report/Group1.pdf> accessed on 20 November 2010

Shetty S, 'Introduction to Spyware Keyloggers' 04-4- 20005 available at <http://www.symantec.com/connect/articles/introduction-spyware-keyloggers> accessed at 10 November, 2010

Song M and Leonetti C, 'The Protection of Digital Information and Prevention of Its Unauthorized Access and Use in Criminal Law' (2011) available at <http://works.bepress.com/carrie_leonetti/14/> viewed on 28 December 2011

Senator Leahy, Statement, Introduction of the 'Anti-Phishing Act Of 2004' 150 Cong, Rec. S7897 (July 9, 2004) [hereinafter Senator Leahy Statement] (statement of Sen. Leahy), available at <http://www.gpo.gov/fdsys/pkg/CREC-2004-07-09/pdf/CREC-2004-07-09PgS7897-2.pdf> viewed on 12 July 2012

Sproule S and Archer N, 'Defining Identity Theft – A Discussing Paper' McMaster eBusiness Research Centre, McMaster University 2006 available at <http://www.business.mcmaster.ca/idtdefinition/IDT%20Discussion%20Paper%20Revision%20from%20Sue%20Sproule%20April%206%2006.pdf> accessed on 1 August 2011

Slapper G, 'The Law Explored: Ignorance of the Law' June 6, 2007 Times of Line 1 available at <http://www.thedogcentre.com/files/Ignorance.pdf> accessed on 11 January 2012

Teague D, Authorities: 'Scam Took Ids of Deceased' (2004) MSNBC News available at <http://www.msnbc,msn.com/id/3899283/ns/nightly_news/t/authorities-scam-took-ids-deceased/> accessed on 25 May 2011

Whitley Edgar A and Hosein Ian R, 'Policy Engagement as Rigourous and Relevant Information Systems Research: The Case of the LSE Identity Project' 2007 London School of Economics and Political Science available at <http://personal.lse.ac.uk/whitley/allpubs/ecis2007.pdf> accessed on 15 February 2011

Wang W J, Yuan Y, and Archer N, 'Identity Theft: A Contextual Framework for Combating Identity Theft' Security and Privacy IEEE 2006 available at <http://see.xidian.edu.cn/hujianwei/papers/014-A%20Contextual%20Framework%20for%20Combating%20Identity%20Theft.pdf> accessed on 28-Oct-2010

Wilson J, 'Confidential Information-Recurrent Problem and Recent Developments' (2009) available at <http://www.11kbw.com/articles/docs/JulianWilsonConfidential_Information.pdf> viewed on 30 December 2011

Whang Insu, 'The Property Concept in Criminal Law, Dissertation of Sungkyunkwan University' (2006)

List of people interviewed

Interview with Dr. A Baaj, Specialist in criminal law and a lecturer at School of law, Baghdad University, School of Law (Baghdad, 30 January 2013)

Interview with Dr. Muhammad Murhij, a Professor of criminal law at Anbar University, School of Law (Anbar, 20 January 2013)

Interview with Dr. assistant Professor S Al Fatlawi, a lecturer and Deputy Head of School of Law, Baghdad University School of Law (Baghdad, 16 February 2013)

Interview with Dr. assist Professor Firas Abdul Moneim and Head of law department at Baghdad University School of Law (Baghdad, 20 February 2013)

Interview with Ahmed Farhan, a criminal judge at Cassation Court, Cassation Court, (Baghdad, 25 January 2013)

Interview with Ali Al-Obeidi, a judge at Federal Court of Appeal of Baghdad Rusafa, (Baghdad 27 January 2013)

Interview with M Al-Zubaidi, a lawyer at Presidency of the Federal Court of Appeal of Baghdad/ Rusafa, (Baghdad, 27 January 2013)

Interview with A Al Obeidi and A Al Ali, lawyers at Presidency of the Federal Court of Appeal of Baghdad/ Rusafa (Baghdad, 27 January 2013)

Interview with M Abdul Ali, Deputy President of Federal Court of Appeal of Baghdad Rusafa, Presidency of Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

Interview with J K Maeen, the Head of the first criminal group in Appeal Baghdad Federal Court, Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

Interview with S Abdul Hadi, a judge at Federal Court of Appeal of Diyala, (Diyala Court, 25 January 2013)

Interview with A Hardan, the Head of Diyala Criminal Court, Presidency of the Federal Court of Appeal of Diyala (Diyala, 5 February 2013)

Interview with Mowaffaq Abdali Deputy President of Federal Court of Appeal of Baghdad/ Rusafa at Presidency of Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

Interview with Khalid Daib, the Deputy President of Federal Court of Appeal of Diyala at Presidency of the Federal Court of Appeal of Diyala (Diyala Court, 26 January 2013)

Appendix 1

List of people interviewed

Interview with Dr. A Baaj, Specialist in criminal law and a lecturer at School of law, Baghdad University, School of Law (Baghdad, 30 January 2013)

Interview with Dr. M Mahrous, a Professor of criminal law at Anbar University, School of Law (Anbar –Haditha, 25 January 2013)

Interview with Dr. Muhammad Murhij, a Professor of criminal law at Anbar University, School of Law (Anbar, 20 January 2013)

Interview with Dr. assistant Professor S Al Fatlawi, a lecturer and Deputy Head of School of Law, Baghdad University School of Law (Baghdad, 16 February 2013)

Interview with Dr. assist Professor Firas Abdul Moneim and Head of law department at Baghdad University School of Law (Baghdad, 20 February 2013)

Interview with Abdul Al-Hamid Al-Taie a lecturer at Diyala University School of law (Diyala- Baquba, 23 February 2013)

Interview with Ahmed Farhan, a criminal judge at Cassation Court, Cassation Court, (Baghdad, 25 January 2013)

Interview with Ali Al-Obeidi, a judge at Federal Court of Appeal of Baghdad Rusafa, (Baghdad, 27 January 2013)

Interview with M Al-Zubaidi, a lawyer at Presidency of the Federal Court of Appeal of Baghdad/ Rusafa, (Baghdad, 27 January 2013)

Interview with M Jassim, a lawyer at Federal Court of Appeal of Diyala (Diyala – Muqdadiyah, 16 February 2013)

Interview with Ahmed Ali, a solicitor at Federal Court of Appeal of Diyala (Diyala, 25 January 2013)

Interview with A Al Obeidi and A Al Ali, lawyers at Presidency of the Federal Court of Appeal of Baghdad/ Rusafa (Baghdad, 27 January 2013)

Interview with M Abdul Ali, Deputy President of Federal Court of Appeal of Baghdad Rusafa, Presidency of Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

Interview with J K Maeen, the Head of the first criminal group in Appeal Baghdad Federal Court, Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

Interview with S Abdul Hadi, a judge at Federal Court of Appeal of Diyala, (Diyala Court, 25 January 2013)

Interview with A Hardan, the Head of Diyala Criminal Court, Presidency of the Federal Court of Appeal of Diyala (Diyala, 5 February 2013)

Interview with Mowaffaq Abdali Deputy President of Federal Court of Appeal of Baghdad/ Rusafa at Presidency of Appeal Baghdad Federal Court (Baghdad, 27 January 2013)

Interview with Khalid Daib, the Deputy President of Federal Court of Appeal of Diyala at Presidency of the Federal Court of Appeal of Diyala (Diyala Court, 26 January 2013)

Interview with: Dr. Bassim Abid Zaman, a criminal judge at criminal Khark Court (Baghdad, 22 February 2013)

Interview with B Obeidi, a prosecutor at Presidency of the Federal Court of Appeal of Diyala, (Diyala Court, 26 January 2013)

Interview with Kadhim Al Taee, a prosecutor at presidency of Federal Court of Appeal of Baghdad Rusafa (Baghdad, 27 January 2013)

Interview with Raad Jubouri, a prosecutor at Iraqi Court of Cassation, Prosecutor Public Service (Baghdad, 22 February 2013)

Appendix 2

The Transcription of the Interview in English Language

The name of interviewee: Dr. Alaa Baaj

Occupation: Specialist in criminal law and a lecturer in the School of law

The place of work: Baghdad University, School of Law

Location of the interview: Baghdad city

The date of the interview: 30th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's mean of identification is not property. It cannot be property. It likes debentures, shares, or patent. It cannot be subject to theft.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I do not believe that the current theft offence laws are adequate to protect this information in itself because the current theft offence laws have been enacted to protect a movable tangible property, whereas people's means of identification is not tangible. The current theft offence laws may protect the physical material that contains people's means of identification. The Iraqi legislation should enact a new law to govern this crime. The law should accompany the technological development.

Q3. Can another person's means of identification be subject to physical taking?

I think physical taking is the important element by which a person's means of identification can be determined whether it is a subject of theft. Scholars have opinions about whether this means of identification can be subject to physical taken. You can decide whether it is subject to the physical taking after examining these views.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

As I stated previous when I answered the first question, a person's means of identification is not property. Consequently, taking it does not deprive the person of it.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that governs identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

No. The criminal judge cannot interpret the current theft offence laws in a manner to govern identity theft. If he interprets existing theft offence laws in a manner that governs identity theft, he will offend the principle of legality that is set forth in the Iraqi legislation.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality prevents the criminal judge from extending the current theft offence laws (or from creating new laws) to govern identity theft.

Q7. To what extent, do you think that Information Crimes Project of 2011 will adequately protect people's means of identifications from the illegal use by other persons?

Information Crimes Project of 2011 is still in infant. If it is enacted in its current formulation, it cannot protect people's means of identification.

Q8. What in your opinion is one the strengths of the 2011 project (to help combat identity theft)?

The project of 2011 cannot combat identity theft. The Iraqi legislature does not directly criminalise identity theft.

Q9. What in your opinion is one the strengths weakness of the 2011 Project (to not help combat identity theft)?

As I stated about the previous question, the strength weakness of the 2011 project is the project of 2011 does not criminalise the taking of another person's means of identification without consent, and then using to commit other crimes.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of crime if so, and what crime?

Yes, they are guilty of crime. They may be guilty of identity theft offence. According to their role, they may be guilty of principal or secondary participants in identity theft.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

Yes, the Iraqi legislator should criminalise these methods and consider them specific crimes because these methods can be used to commit other crimes rather than identity theft.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

Yes, it should be a crime in itself. However, the legislator sometimes criminalises the forging or imitating of another person's signature or the using of his name.

The name of interviewee: Dr. Muhammad Murhij

Occupation: A Professor of criminal law

The place of work: Anbar University, School of Law

Location of the interview: Anbar city

The date of the interview: 20th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

Intangible materials, such as computer programs and information like intellectual opinions or what is called intellectual property are not tangible things. It likes intangible things. Therefore, they are not property. They also are not subject to theft. I have a published article that carries the name "difficulties that may be faced when the Iraqi theft offence laws applied to computer programs."

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I do not think that the current theft offence laws can be applied to identity theft. They were enacted to deal with and protect the tangible property only.

Q3. Can another person's means of identification be subject to physical taking?

Generally, the information cannot be subject to physical taking because just the tangible property can be subject to physical taking. However, when a person's means of identification has been taken from internet or individuals' computers that is connected with the internet it can be subject to physical taking like electricity power.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, the owner is not permanently deprived of his information. He still uses it, although another person without consent uses it

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

In general, the criminal judge cannot interpret the current theft offence laws in a manner that governs identity theft because if he interprets them in a manner that governs identity theft, he violates the principle of legality. In my opinion, due to these crimes are new the judge should interpret existing theft offence in a manner governs them until the Iraqi legislatures enacts a new act to govern modern crimes.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, which can prevent the criminal judge from extending existing theft offence laws (or from creating new laws) to cover identity theft.

Q7. To what extent, do you think that Information Crimes Project of 2011 will adequately protect people's means of identifications from the illegal use by other persons?

The project of 2011 is insufficient to govern identity theft. It does not directly criminalise identity theft. The judge may find it difficult to apply this project to identity theft.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)?

I do not find strengths in the 2011 project can help combat identity theft.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I think that one the strengths weakness is the Iraqi legislature does not criminalise identity theft as a crime in itself. It should add to this project an article that directly deals with identity theft.

Q10. Where bank workers, government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

Bank workers, government officials, or internet providers are considered participants in identity theft either as principal or secondary participants.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

Yes, I think that sophisticated methods should be criminalised as crimes in themselves because criminals sometimes use these methods to affect and destroy people computers or to commit other crimes, such as fraud. Therefore, it is necessary to consider these methods as crimes in themselves.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that the obtaining of another person's means of identification should be criminalised as a crime in itself. Considering the theft of identity as a crime in itself is more important to combat the illegal use of another person's means of identification to commit other crimes.

The name of interviewee: Firas Abdul Moneim

Occupation: assist Professor and Head of law department at Baghdad University School of Law

The place of work: Baghdad University-School of Law

Location of the interview: Baghdad

The date of the interview: 20th of February 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I do not think that people's means of identification is property. It has no value. It cannot be subject to sell or rent. It is an intangible thing.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think taking another person's means of identification, and then using it to commit other crimes is not theft. People's means of identification is never being subject to theft.

The term theft is limited to tangible things only. Therefore, I do not discuss the issue whether the current theft offence laws are adequate to cover identity theft or not.

Q3. Can another person's means of identification be subject to physical taking?

No, people's means of identification cannot be subject to physical taking because it is intangible. Tangible things only can be subject to physical taking.

The interviewer said to him that Iraqi legislatures did not define the term appropriation, do you think that the term appropriation should occur by a physical action only. He answered yes. However, during his speech he said there is no specific means to appropriate another person's property. The interviewer is confused and cannot determine the interviewee's opinion about whether the means of identification can be subject to physical taking or not.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, taking of another person's means of identification does not permanently deprive him of the ownership of his identity.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the criminal judge cannot interpret the current theft offence laws in a manner that governs an illegal act, which the Iraqi legislature has not previously considered it as a crime.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the criminal judge from extending existing theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in them.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?
I have not read it yet.
Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)
I cannot comment on it because I did not read it.
Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?
I cannot comment on it because I did not read it.
Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?
I think that bank workers and internet providers are guilty of participation in identity theft either principal or secondary participants.
Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?
I do not think that sophisticated methods need to be crimes in themselves. These methods are means to commit identity theft. Criminalising identity theft encompasses both the crime, and the means that is used to commit it.
Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?
I think that the illegal obtaining of another person's means of identification, and then use it to commit other crimes needs to be a crime in itself.

The name of interviewee: Dr. assistant Professor Salah Al Fatlawi
Occupation: A lecturer and Deputy Head of School of Law
The place of work: Baghdad University School of Law
Location of the interview: Baghdad- School of Law
The date of the interview: 16th of February 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is a right that is considered closely to the person, but it is not property. It belongs to him, but it is not property.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think that obtaining people's means of identification, and then using it to commit other crimes is not theft because a person means of identification is not property. It cannot be subject to theft.

Q3. Can another person's means of identification be subject to physical taking?

No, taking another person's means of identification cannot be subject to physical taking. Seeing, hearing or copping this means does not fall within the scope of physical taking that is required by the Iraqi legislature in the current theft offence laws.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, the taking of another person's means of identification does not deprive that person of his identity. He still uses it.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the Iraqi criminal judge cannot interpret the current theft offence laws in a manner that covers identity theft. The judge cannot create a crime or determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating a new law) to overcome the inadequacy that may appear in them.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I have not read it yet.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I cannot comment on it.

Q10. Where bank workers, government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by

intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think that bank workers, government officials, or internet providers are guilty of participation in identity theft. According to their roles, they may be guilty in either principal or secondary participations in identity theft.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that sophisticated methods need to be crimes in themselves because criminalising crimes that are committed by using these methods is not enough to deter unscrupulous people. Enacting a new law to criminalise them is necessary.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that the obtaining of another person's means of identification need to be a crime in itself. The Iraqi legislature should enact a new law to govern the illegal obtaining of people's means of identification, and then using it to commit other crimes.

The name of interviewee: Dr. Mohammad Mahrous

Occupation: A Professor of criminal law

The place of work: Anbar University, School of Law

Location of the interview: Anbar -Haditha

The date of the interview: 25th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and

may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think we should distinguish between a confidential person's means of identification or financial information, such as PIN number and non-confidential identification, such as the person's address or his name. The confidential identification is property and it may be subject to theft, but non-confidential identification is not property and it may not be subject to theft.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

No, I think that the current Iraqi theft offence laws are inadequate to protect individuals' means of identification because these laws were enacted to govern the tangible property only whereas individuals' identification is intangible.

Q3. Can another person's means of identification be subject to physical taking?

I think that a person's means of identification can be subject to taking, but not physical taking like tangible property. It can be subject to taken through seeing, hearing or copying it.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

Yes, taking of another person's means of identification without his consent can permanently deprive him of his identification. The person's whose identity has been stolen will lose his money and his reputation will be affected if this means has been used to commit other crimes.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the criminal judge cannot extend the scope of the current theft offence laws through interpretation (or create new laws) to govern identity theft. He cannot determine a crime and set out a punishment for it.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, it constitutes an obstacle that prevents the criminal judge from extending the current theft offence laws (or from creating new laws) to overcame the inadequacy that may appear in them to cover identity theft. However, it is necessary because it respects the separation powers and protects people from the judge arbitrariness.

Q7. To what extent, do you think that Information Crimes Project of 2011 will adequately protect people's means of identifications from illegal use by other persons?

I think that the 2011 project has many flaws that may make it inadequate to protect people's means of identification.

Q8. What in your opinion is one the strengths of the 2011 project (to help combat identity theft)?

I think that the 2011 project has no strengths to help combat identity theft.

Q9. What in your opinion is one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I think it does not contain provisions to protect people's means of identification and combat identity theft.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think that a bank worker, government official and internet provider may be guilty of participation in identity theft either as a principal or secondary participant as long as he knows that those people to whom he sells the means of identification will use it to commit other crimes.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that sophisticated methods, (such as phishing or spam) are widely used by criminals to commit identity theft or other crimes, therefore, it is important if to these methods are being considered as crimes in themselves.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that identity theft should be criminalised either as a crime in itself or as a method that may be used to commit other crimes.

The name of interviewee: Abdul Al-Hamid Al-Taie

Occupation: A lecturer

The place of work: Diyala University- School of law

Location of the interview: Diyala- Baquba

The date of the interview: 23rd of February 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may

arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is property and it can be subject to theft.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I do not think that the current theft offence laws are adequate to govern identity theft and protect individuals' means of identification because they were enacted to govern the tangible property only.

Q3. Can another person's means of identification be subject to physical taking?

No, a person's means of identification cannot be subject to physical taking. It can be subject to non-physical taking. It can be obtained by seeing, hearing, and then memorising or by copying

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

I do not think that the taking of another person's identification (without his consent to use it to commit other crimes) deprives him of it.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

The criminal judge cannot interpret existing theft offence laws in a manner that governs identity theft. If he interprets and extends the scope of these laws to govern identity theft, he offends the principle of legality.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle that prevents the criminal judge from extending the current theft offence laws (or from creating new laws) to cover identity theft. We sometimes cannot consider an act as a crime even if we are convinced that it is a crime because the legislator did not consider it as crime.

Q7. To what extent, do you think that Information Crimes Project of 2011 will adequately protect people's means of identifications from the illegal use by other persons?

I do not think that Information Crimes Project of 2011 will adequately protect people's means of identification from the illegal use by other persons.

Q8. What in your opinion is one the strengths of the 2011 project (to help combat identity theft)?

In my opinion, there is no one the strengths in this project can help combat identity theft.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

In my opinion, one the strengths weakness in the 2011 project is it does not contain rules that can help combat identity theft.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think that a banker worker, government official or internet provider involves in participation in identity theft either as a principal or secondary participant.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that these methods need be crimes in themselves.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? On the other hand, should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?
I think that identity theft needs to be a crime in itself. The criminal judge can prosecute the accused on both identity theft and other crimes that are committed by using it and enforce a strictest sentence.

Lawyers
The name of interviewee: Mahdi Al-Zubaidi
Occupation: A lawyer
The place of work: Presidency of the Federal Court of Appeal of Baghdad/ Rusafa
Location of the interview: Baghdad/ Court of Appeal of Baghdad/ Rusafa
The date of the interview: 27th of January 2013
First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.
Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is not property. Yes, it belongs to that person, but it is not property. There is difference between the property and the personal right. The means of identification is a right, but it is not property.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think that the use of people's means of identification is not theft. It is false representation or forgery. If this means is not used to commit other crimes it constitutes a preparatory action for commissioning of other crimes, and the preparatory action is not a crime according to Iraqi legislation.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's means of identification cannot be subject to physical taking. The term appropriation that is stated in the Iraqi Penal Code 1969 occurs when a person physically takes another person property. However, it does not occur when the person sees, hears, and then memorises, or copies the person's means of identification.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, the owner is not permanently deprived of his means of identification when it has been taken by another person. There is moral damage. His reputation is wrecked, and this may be equal to permanent deprivation.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the criminal judge cannot interpret the current theft offence laws to govern identity theft because he cannot create a new crime and determine a punishment for it.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle and prevents the judge from extending existing theft offence laws (or from creating new laws) to govern identity theft.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I have not read it yet.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I cannot comment on it.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think those persons are guilty of participation in either principal or secondary participants in identity theft.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that sophisticated methods need to be crimes in themselves, particularly some of them related to the internet, and we have no act that may be used to protect our online transactions.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I do not think that the obtaining of another person's means of identification needs to be a crime in itself. If it is used to commit another crime, it is considered a means to commit this crime, and the means that is used to commit other crimes is unnecessary to

be criminalised. Prosecuting the accused on the crime that has been committed only is enough to deter other persons.

The name of interviewees: Ali Al Obeidi and Amer Al Ali
Occupation: lawyers
The place of work: Presidency of the Federal Court of Appeal of Baghdad/ Rusafa
Location of the interview: Federal Court of Appeal of Baghdad/ Rusafa
The date of the interview: 27th of February 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

We think that person's means of identification is not property, but it belongs to the person who uses it.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

We think that using another person's means of identification is false representation. It is not theft. Consequently, the current theft offence laws unsuitable to apply to a person who uses another person's means of identification to commit other crimes.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's means of identification cannot be subject to physical taking.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, the taking of another person's means of identification does not deprive that person of his identity.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

We think that the criminal judge can interpret existing theft offence laws to explore the aim of the legislation, but he cannot create a new crime or determine a punishment for it.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the judge from extending the current theft offence laws to overcome the inadequacy that may appear in them.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

We have not read it yet. However, we consider this action a good step that has been taken by the Iraqi legislature.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

We cannot comment on it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

We cannot comment on it.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

We think that bank workers or internet providers are guilty of participation in identity theft.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

We think that sophisticated methods need to be crimes in themselves because some of this means may be crimes in themselves.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

We think that the obtaining of another person's means of identification needs to be a crime in itself. The legislature should criminalise both the obtaining of the means of identification and the crime that is committed by using it, and then the criminal court will enforce the hardest punishment upon him.

The name of interviewee: Muhammad Jassim

Occupation: A lawyer

The place of work: Federal Court of Appeal of Diyala

Location of the interview: Diyala - Muqdadiyah

The date of the interview: 16th of February 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with

giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I do not think that a person's means of identification is property. Some elements should be available in a thing to be property, such as the thing should be tangible, it has value, and it is subject to possession. However, the identity of person cannot be a subject to possession.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

A person's identity cannot be a subject of theft because it is not property. However, if it is considered property and it can be subject to theft the current theft offence laws are inadequate to govern it because these laws were enacted to govern tangible property only.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's mean of identification cannot be subject to physical taking. A physical thing, such as a car other his tangible properties only can be subject to physical taking. If somebody takes it he may be guilty of theft. The intangible methods, such as copying, seeing, or hearing that are used to obtain people's means of identification cannot fall within the scope of physical taking.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

I do not think that taking of another person's means of identification deprives the person of it. The theft offence as it is defined means appropriation the possession from the owner with intent permanently to deprive him of it, but this does not happen when the person takes another person's means of identification. The accused shares the person in his identity only. The person still possesses and uses his identity.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the judge should respect the principle of legality. He should not interpret the existing theft offence laws in a manner that may lead to extend them or create a new law to cover identity theft. By not doing so, he may offend the principle of legality.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, it does. However, it is necessary to prevent the judge from usurping the legislator function. The legislator should be the only one enacts laws. If there is lack in the legislation the judge should inform the legislature that there is lack in the legislation, and then the Iraqi legislature could amend the law or abolish it.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from the illegal use by other persons?

The Information Crimes Project 2011 is great achievement that has been done by the Iraqi legislature, but it is inadequate to protect people's means of identification of the illegal use by the unscrupulous persons.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I hope there is one strengths in the 2011 project that can help combat identity theft, but it is not.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

The one strengths weakness that I can find it in the 2011 project is it does not directly govern identity theft. It should contain article deals directly with identity theft.

Q10. Where a bank worker or government official or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think they are involved in participation in identity theft. According to Iraqi legislation, the participation means a person is guilty of participation in a crime if he aids, abets, or instigates another person to commit a crime. They may be guilty of participation in identity theft either principal or secondary participants.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think this issue should be decided by the legislator because it the only one can decide whether these methods need to be crimes in themselves or not. I think there are some methods more serious than other methods. Consequently, the legislator should determine which methods be crimes in themselves.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that the obtaining of another person's means of identification should be a crime in itself. It is a dangerous tool, which the criminal can use to exhaust the victims money. It should be criminalised like possession of an artificial key.

The name of interviewee: Ahmed Ali

Occupation: A solicitor

The place of work: Federal Court of Appeal of Diyala

Location of the interview: Diyala

The date of the interview: 25th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is not property. It is impossible another person's means of identification (such as his name or date of birth) to be considered property like tangible property. It does not belong to the person. It has no value. It cannot be subject to possession.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think that the obtaining of another person's identity can never be theft as the obtaining of tangible property. People's means of identification cannot be subject to theft because some people use the same means of identification. A person who uses a name rather than his name may be guilty of forgery or false representation. He should use his name as it is recorded in government documents.

Q3. Can another person's means of identification be subject to physical taking?

No, it cannot be subject to physical taking. If a person uses the identity of another person to avoid arrest by the police he commits forgery or uses documents that belong to another person.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, there is no permanent deprivation to the person of his identity. He still uses it. As I said a person's means of identification is not property, consequently the person who has a right in this means is not deprived of it if it is used by another person.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the judge cannot interpret existing theft offence laws to cover identity theft. He should apply these laws as they have been enacted. According to the principle of legality, crimes and their punishments should be determined by the legislature.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle. The judge cannot consider an act as a crime (identity theft) because the principle of legality obliges him and prevents him from creating a crime.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I think that Project of 2011 is important step that has be conduct by the Iraqi legislature because the existing criminal law was enacted to govern crimes during a period of time there was no internet. Nowadays, many crimes can be committed via the internet. The existing criminal law is inadequate to combat these types of crimes. The Iraqi legislature should fill the gap in the legislation through enacting new laws like this.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

The main aim of this project is not to criminalise or combat identity theft. The legislator intends to limit the use of the internet. The legislator also intends to prevent some act that may commit against the regime.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

This project does not criminalise the use of a person's means of identification to commit other crimes. As I said the obtaining another person's means of identification is not theft, but the legislator should add an article in this project to inform people that the use of person's identity to commit other crimes is a crime.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

Internet providers or government officials and non-government officials are guilty of participation in information theft offences because they can easily obtain this information without an obstacle. They should be principal participants in these crimes.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I do not think that these methods need to be crimes in themselves because criminalising the crime will also include methods that are used to commit it. It is unnecessary to criminalise everything that surrounds the crime committing. Criminals also develop their methods to overcome obstacles that may face them.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that the obtaining of another person's means of identification should be a crime in itself, but not theft. The legislator should determine whether it is theft or fraud. People should be immune when they use the internet or their credit or debit card.

Judges

The name of interviewee: Ahmed Farhan

Occupation: A criminal judge at Cassation Court

The place of work: Cassation Court

Location of the interview: Baghdad

The date of the interview: 25th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I do not think that people's means of identification is property.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I agree with my colleague Mr. Hassan that the illegal taking of another person's means of identification is not punished as a crime unless it is used in illegal purposes, such as fraud or theft of money from a bank. In this case, the accused should be punished on the

crimes, such as fraud, forgery, or theft of money that are committed by using a person's means of identification.

Q3. Can another person's means of identification be subject to physical taking?

No, it cannot be subject to physical taking.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, the taking of another person's identification does not deprive him of it. He still uses it, although somebody else can use it.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that governs identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I do not think that the Iraqi criminal judge can interpret existing theft offence laws in a manner that covers identity theft. He can extend the meaning of them to explore the intention of the legislator to apply these laws correctly, but he cannot extend them to govern identity theft.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, it constitutes an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in them.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I have not read it yet. However, I think it is better than nothing.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

Sorry, I told you that I did not read it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

It is the same answer.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

Those persons are guilty of participating either principal or secondary participation of in identity theft.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I do not think that sophisticated methods if they are used to obtain another person's means of identification need to be crimes in themselves. However, they may be crimes in themselves if they are used to destroy the integrity of the computers.

12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I do not think that identity theft needs to be a crime in itself because criminalising the illegal activities that are committed by using another person's means of identification is enough to deter unscrupulous persons and protect it.

The name of interviewee: Ali Al-Obeidi

Occupation: President of Federal Court of Appeal of Baghdad/ Rusafa

The place of work: Federal Court of Appeal of Baghdad Rusafa

Location of the interview: Baghdad

The date of the interview: 27th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with

giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is property. It is personal rights.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

Actually, according to the purpose that people's means of identification is used to achieve, it is subject to many legal texts and not just theft offence laws.

Q3. Can another person's means of identification be subject to physical taking?

Yes, another person's means of identification can be subject to physical taking.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, the owner is not permanently deprived of it. The illegal use of another person's means of identification to commit other crimes constitutes a civil action, and not a criminal action.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has

been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the criminal judge can interpret existing theft offence in a manner that leads to explore the purpose of them only. Therefore, the interpretation may be narrow or extensive according to the purpose of these laws. However, the criminal judge cannot interpret them to create a crime (identity theft) and consequently determine a punishment for it.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the criminal judge from extending the current theft offence laws.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I have not read it yet.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on this Project because I did not read it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

The same answer I have not read it yet.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think they are participants as the principal actor. They are criminals.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I do not think that there is necessary to criminalise sophisticated methods that are used to commit identity theft because the crime and sophisticated methods, which are used, constitute one criminal enterprise

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

Yes, it is necessary to enact a new law to criminalise the obtaining of another person's means of identification to commit other crimes.

The name of interviewee: Mowaffaq Abdali

Occupation: Deputy President of Federal Court of Appeal of Baghdad/ Rusafa.

The place of work: Presidency of Appeal Baghdad Federal Court.

Location of the interview: Baghdad

The date of the interview: 27th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is property. It is mine and belongs to me.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I do not think that the current theft offence laws are adequate to govern identity theft and protect people's means of identification.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's means of identification cannot be subject to physical taking. The taking should be in physical action, not in hearing, coping or seeing the thing, but the use of it without the person's consent constitutes a crime.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, taking of another person's means of identification does not permanently deprive him of it.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the criminal judge can expansively interpret existing theft offence laws to explore the spirit of them, but he cannot create a crime and determine a punishment for it. Consequently, the Iraqi criminal judge cannot consider the obtaining of another person's means of identification without his consent as theft.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the criminal judge from extending existing theft offence laws to overcome the inadequacy that may appear in.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I think the Project of 2011 is a good step that is taken by the Iraqi legislature. A thing is better than nothing.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on the Project of 2011 because I did not read it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I give you the same answer.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

Sure, they are participants in identity theft.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I do not think that sophisticated methods need to be crimes in themselves because criminalising identity theft contains both the crime and the means that is used to commit it.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think the Iraqi legislature should enact a new law to criminalise the obtaining of another person's means of identification. It is not enough to criminalise the crimes that are committed by using the person's means of identification. The criminal judge can prosecute the accused on both obtaining the means and the crime that is committed by using it, and then enforce the strength punishment upon the accused.

The name of interviewee: Jawad Khalid Maeen

Occupation: Head of the first criminal group in Appeal Baghdad Federal Court

The place of work: Appeal Baghdad Federal Court

Location of the interview: Baghdad

The date of the interview: 27th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I do not think that a person's means of identification is property. It is shapeless and has no value, so it is not property.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think taking another person's identification is not a crime because the crime is an illegal activity that is committed against people's bodies or their property, whereas the means of identification is not a part of body or property. Therefore, I do not think that the current theft offence laws are adequate to govern identity theft because they were enacted to govern movable property only.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's means of identification is not property and cannot be subject to physical taking or transferring.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, taking another person's means of identification does not permanently deprive him of it.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

No, I do not think that the criminal judge can interpret existing theft offence laws in a manner that governs identity theft because the principle of legality prevents him from doing so.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality prevents the criminal judge from extending the current theft offence laws (or creating new laws) to overcome the inadequacy that may appear in them.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect people's means of identifications from the illegal use by other persons?

Yes, the project of 2011 can protect people's means of identification from the illegal use by other persons.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I have not read it yet, but I think that one may find a legal text, which can be used to combat identity theft.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I did not read it.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?
They are participants in either principal or secondary participation according to their roles in identity theft commission. According to the rules of participation in Iraqi Penal Code, they may be subject to the same punishment that is set out to the principal actor.
Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?
I think that sophisticated methods should be considered crimes in themselves when they are used to commit other crimes. However, they do not need to be crimes in themselves if they are not used to commit other crimes.
Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?
I think that it is necessary to enact a new law to cover identity theft because criminalising crimes that are committed by using people's means of identification is inadequate to protect this means of identification.

The name of interviewee: Ali Hardan
Occupation: Head of Diyala Criminal Court
The place of work: Presidency of the Federal Court of Appeal of Diyala
Location of the interview: Diyala
The date of the interview: 5th of February 2013
First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD

thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I do not think that a person's means of identification is property. It does not belong to him. I think that national identity cards are used Iraq. Taking a person's identity card constitutes theft because the "identity card" is property. In addition, using another person's means of identification may constitute false representation, but not theft.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think that taking another person's means of identification is not theft because it is not property. However, in our view existing theft offence laws are inadequate to accompany with the technological development. The Iraqi Penal Code was enacted in 1969, and the world now in 2013. There is huge difference between the life in 1969 and the life now. For instance, terrorists can use different means to commit their crimes and kill many people. In the past, these means were unknown to the Iraqi legislature. Therefore, the Iraqi legislature enacted the Terrorism Act 2005 to combat terrorism operations. We need a new law to deter unscrupulous persons and protect people.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's means of identification is not property, but it becomes property if it has shape and size. Just in this case, it may be subject to physical taking.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

Yes, the taking of another person of identification permanently deprives the owner of his means of identification. In this case, the accused may be prosecuted on theft according to article 439 of the Penal Code 1969, fraud or betrayal trust when the accused take his fellow's means of identification or the means of identification of any person who has relationship with him.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

The criminal judge cannot interpret the current existing theft offence laws in a manner that governs identity theft, even if he does not find specific legal texts. He should interpret the current theft offence laws to determine whether identity theft falls within the scope of them or not. If he discovers that identity theft does not fall within the scope of these laws, he cannot apply them on it.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the criminal judge from extending the current theft offence laws (or creating new laws) to overcome the inadequacy that may appear in existing theft offence laws.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I have not read it yet.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on it because I did not read.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I did not read it.

Q10. Where a bank worker or government official or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?
Workers in the bank and the providers are guilty of forgery because they forge the data according the rules of the law of the Iraqi Central Bank 2004. In addition, they are guilty of disclose the secret information crime that is stipulated in article 327 of the Iraqi Penal Code 1969.
Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?
I think the current Iraqi Penal Code rules are adequate to govern sophisticated methods, but the punishment should be changed if these methods used to steal a huge amount of money.
Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?
Yes, identity theft needs to be a crime in itself. In our opinion, most laws need reform and change the punishments, or enact new laws to accompany with technological development.

The name of interviewee: Saad AbdulHadi
Occupation: A judge
The place of work: Federal Court of Appeal of Diyala
Location of the interview: Diyala Court
The date of the interview: 25th of January 2013
First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University,

School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that another person's means of identification is not property. It is a personal right.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think that using another person's means of identification to commit other crimes is not theft. If this means used to commit other crimes, it is considered a means to commit other crimes. In the criminal law, the means is not considered as a crime. Consequently, if the criminal uses another person's means of identification to commit other crimes, he may be subject to other legal texts, such as fraud or forgery.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's means of identification cannot be subject to physical taking.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, taking of another person's means of identification does not permanently deprive that person of his means of identification.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of

existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think the Iraqi criminal judge can interpret the current theft offence laws to explore the spirit of them irrespective whether the interpretation is narrow or expansive, but he cannot create a new law to govern identity theft. The Iraqi legislature has determined many crimes in the Penal Code 1969, thus, the judge cannot create a new crime and set a punishment for it if it is not stipulated in the current Penal Code.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the judge from extending existing theft offence laws (or creating new laws) to overcome the inadequacy that may appear in them.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I have not read it yet.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on it because I did not read it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I cannot comment on it.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think that bank workers or internet providers are considered participants in identity theft.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in

themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I do not think that sophisticated methods need to be crimes in themselves because identity theft and the methods that are used to commit it constitute one criminal enterprise.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think the obtaining of another person's means of identification needs to be a crime in itself because criminalising crimes that are committed by using stolen means of identification is inadequate to deter identities thieves.

The name of interviewee: Khalid Daib

Occupation: Deputy President of Federal Court of Appeal of Diyala

The place of work: Presidency of the Federal Court of Appeal of Diyala

Location of the interview: Diyala Court

The date of the interview: 26th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your

personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person means of identification is property.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think that the current theft offence laws are inadequate to cover identity theft because they were enacted to deal with tangible property only. The Iraqi legislature should enact a new law to protect people means of identification.

Q3. Can another person's means of identification be subject to physical taking?

I do not think that people's means of identification can be subject to physical taking.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, the taking of another person's means of identification does not permanently deprive him of it. He still uses his means of identification.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I do not think that the criminal judge can interpret the current theft offence laws in a manner that may cover identity theft.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the criminal judge from extending existing theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in them to govern identity theft.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I think that the Project of 2011 is a good step.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on it because I have not read it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I cannot comment on it.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think that they are guilty of participation in identity theft.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that sophisticated methods need to be crimes in themselves, and the Iraqi legislature should enact a new law to criminalise them.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that identity theft needs to be a crime in itself.

The name of interviewee: Dr. Bassim Abid Zaman

Occupation: A criminal judge

The place of work: Criminal Khark Court

Location of the interview: Baghdad city

The date of the interview: 22nd of February 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with

giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is property. A person possesses his name, address and his social security number. He can use and enjoys his means of identification as his car. The means of identification has value, thus, some people want to obtain it.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think that the current theft offence laws are inadequate to govern identity theft. These laws limit the protection to the tangible property and electricity power. We as judges cannot gauge stealing another person's means of identification on stealing the electricity power because the analogy is prohibited by the principle of legality.

Q3. Can another person's means of identification be subject to physical taking?

Another person's means of identification can be subject to taking, but it not physically be taken it can be taken in non-physically manner, such as seeing, hearing, and then memorising, or copying it.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, taking of another person's identification does not deprive him of his identification.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that the criminal judge cannot interpret existing theft offence laws in a manner that governs identity theft, even if he cannot find a specific legal text to govern it.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle that prevents the criminal judge from extending the current theft offence laws (or creating new laws) to govern identity.

Q7. To what extent, do you think that Information Crimes Project of 2011 will adequately protect people's means of identifications from the illegal use by other persons?

Although, there is negation inside Iraqi Parliament about the 2011 project, in my opinion it will not adequately protect people's means of identification from the illegal use by other persons.

Q8. What in your opinion is one the strengths of the 2011 project (to help combat identity theft)?

In my opinion, the 2011 project has no strengths can help combat identity theft.

Q9. What in your opinion is one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I think that one the strengths weakness of the 2011 project is it does not contain rules that can be used to combat identity theft.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

If we apply the general rules of participation on a bank worker, government official or an internet provider's behaviour we may find him guilty of participation in identity theft either as principal or secondary participant.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that it is important to consider sophisticated methods as crimes in themselves.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that the obtaining of another person's means of identification needs to be a crime in itself because it is considered as a key to commit other crimes.

Prosecutors

The name of interviewee: Bidoor Al-Obeidi

Occupation: A prosecutor

The place of work: Presidency of the Federal Court of Appeal of Diyala

Location of the interview: Diyala

The date of the interview: 26th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the

illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is a personal right. It belongs to the person who has a right to use it. Using it without the person's consent is considered a crime.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think the obtaining of another person's means of identification without his consent, and then using it to commit other crimes constitutes fraud not theft. Thus, I think it is unnecessary to discuss whether the current theft offence laws are adequate to govern identity theft or not.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's means of identification cannot be subject to physical taking.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, the taking of another person's means of identification does not permanently deprive him of it.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I do not think that the criminal judge can interpret the current theft offence laws in a manner that governs identity theft because he cannot create a new crime and consequently determine a punishment for it. However, he can interpret these laws to explore the aim of them only.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitute an obstacle and prevents the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in them.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

I have not read this project. However, I consider it a good step that has been taken by the legislature.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on it because I did not read.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I cannot comment on it.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think that those people are considered principal participants in identity theft if they sell this information to other persons or use it to commit other crimes.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that sophisticated methods need to be crimes in themselves. The Iraqi legislature should enact a new law to prevent the misuse of a computer.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that criminalising crimes that are committed by using another person's means of identification is considered enough to deter people because the means of identification is considered a means to commit these crimes. Punishing criminals who use other persons' means of identification to commit other crimes is enough to deter other people.

The name of interviewee: Kadhim Al Taee

Occupation: A prosecutor

The place of work: presidency of Federal Court of Appeal of Baghdad Rusafa

Location of the interview: Baghdad

The date of the interview: 27th of January 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I do not think that a person's means of identification is property. It cannot be described as property.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I think that taking another person's means of identification is never described as theft. Consequently, it is unnecessary to discuss whether the current theft offence laws are adequate to cover identity theft or not. It may be subject to forgery, false representation, or justice misleading.

Q3. Can another person's means of identification be subject to physical taking?

No, another person's means of identification cannot be subject to taking or transferring.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

No, another person's means of identification is not property and cannot be subject to theft, thus, taking it does not deprive the person of it.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think that if the Iraqi criminal judge does not find a specific legal text to cover identity theft he cannot interpret the current theft offence laws in a manner that governs identity theft (or create new laws). He may interpret the existing to explore the spirit of these laws, but he cannot create a new law.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating a new law) to overcome the inadequacy that may appear in these laws.

Q7. To what extent, do you think that Model Information Crimes Project of 2011 will adequately protect peoples' means of identifications from illegal use by other persons?

Although I did not read it, but I think it is a good step that is taken by the Iraqi legislature.

Q8. What in your opinion one the strengths of the 2011 project (to help combat identity theft)

I cannot comment on it because I did not read it.

Q9. What in your opinion one the strengths weakness of the 2011 Project (to not help combat identity theft)?

I give you the same answer.

Q10. Where bank workers, government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think bank workers, government officials, or internet providers are guilty of participation in identity theft. Definitely, they are participants in the crime.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that sophisticated methods need to crimes in themselves.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that identity theft needs to be a crime in itself. Criminalising crimes that are committed by stolen means is inadequate to deter unscrupulous individuals and protect people's means of identification.

The name of interviewee: Raad Jubouri

Occupation: A prosecutor at Iraqi Court of Cassation

The place of work: A Prosecutor at Public Service

Location of the interview: Baghdad

The date of the interview: 22nd of February 2013

First of all, I would like to express my thanks and appreciation for granting me this opportunity to achieve this interview, which will assist me greatly to complete the requirements of my PhD thesis. The information that will be gained from this interview will enrich my thesis. In fact, it will provide an invaluable insight into your work

experience in the field of the application of criminal law. Let our interview start with giving a brief idea about me and my work, I am a PhD candidate at Bangor University, School of Law (United Kingdom). I am in the third year of my period study. My PhD thesis concern deals with an issue that has recently appeared in the world in general and may be in Iraq particularly. This issue is the legal and illegal obtaining of another person's means of identification or their financial information and then using it to commit other crimes. The aim of this interview is to discuss some issues, which may arise when this crime happens in Iraq. As you know there is no specific law that deals with or covering this crime in Iraq. The lack of specific provisions deal with the illegally or legally obtaining of another person's means of identification gives rise to several questions which I would like to discuss with you. Before we start our interview, I would like to receive your consent for the interview, and I can confirm that all your personal details will remain confidential.

Q1. My first question is: Do you think that a person's means of identification is property?

I think that a person's means of identification is not property, but it should be considered property. If we do not accept that a person's means of identification as property we cannot protect it from the illegal use by other persons. By doing so (we do not accept a person's means of identification is property), we ignore the technological development. If there is no law that may be used to protect people's identity they never accomplish their transactions online. They will crow in government institutions, such as banks to accomplish their transactions in traditional manners.

Q2. Do you think that the current theft offence laws in Iraq are adequate to govern identity theft and protect individuals' means of identification?

I do not think that the current theft offence laws are adequate to govern identity theft because these laws were enacted to deal with theft of tangible property only. The Iraqi legislator should amend them.

Q3. Can another person's means of identification be subject to physical taking?

The term physical taking is inadequate to refer to obtaining another person's means of identification because this term uses when tangible property is physically taken. A person's means of identification can be taken, but not physically. It can be taken by non-physical methods, such as seeing, hearing and then memorising, or copying it.

Q4. Does the taking of another person's identification (without his consent to use it to commit other crimes) means that the owner is permanently deprived of the ownership of his identity?

I think there is no actual permanent deprivation to the person of his identity. However, there are some actions may be equal to the permanent deprivation. For instance, a person is permanently deprived of his money if his identity is used to steal this money. In addition, his reputation may be wrecked if his identity is also used to avoid criminal record.

Q5. If the criminal judge cannot find a specific legal text to protect the individuals' identity do you think that the judge can interpret existing theft offence laws in a manner that govern identity theft? In other words, can the criminal judge extend the scope of existing theft offences law in Iraq so that he can determine a crime (identity theft) has been committed and consequently determine a punishment for it even though we do not yet have specific laws in Iraq to govern identity theft?

I think if the Iraqi criminal judge does not find a specific legal text that can be used to govern identity theft he can widely interpret them and extend their scope to govern identity theft, until existing theft offence laws are amended by the legislature.

Q6. Does the principle of legality constitute an obstacle, preventing the criminal judge from extending the current theft offence laws (or from creating new laws) to overcome the inadequacy that may appear in existing laws to cover identity theft?

Yes, the principle of legality constitutes an obstacle that may prevent the criminal judge from extending the current theft offence laws (or from creating new laws) to govern identity theft. In my opinion, criminal judges should be given discretion to interpret criminal statutes widely to make them accompanied with technological development.

Q7. To what extent, do you think that Information Crimes Project of 2011 will adequately protect people's means of identifications from illegal use by other persons?

I think this question is a good example about what I suggested when I answered your previous question. The 2011 Project is inadequate to govern identity theft. If this project comes into force, the criminal judge can widely interpret it to make it adequate to govern identity or he requires the legislature to enact a new Act.

Q8. What in your opinion is one the strengths of the 2011 Project (to help combat identity theft)?

In my opinion, this project does not encourage one to find any strengths in to help combat identity theft.

Q9. What in your opinion is one the strengths weakness of the 2011 Project (to not help combat identity theft)?

In my opinion, the 2011 Project should contain provisions that directly protect people's means identification and help combat identity theft.

Q10. Where bank workers or government officials or internet providers may be participants (either as principal or secondary participants) in identity theft by intentionally and knowingly disclosing or selling identity information to other people who may use it to commit other crimes, are they guilty of a crime if so, and what crime?

I think that a banker worker, government official or internet provider is guilty of participation in identity theft. According to his role in commission identity theft, he may be guilty of participation in identity theft either as a principal or secondary participant.

Q11. Do you think that sophisticated methods (such as phishing or spam) that are used by criminals to obtain another persons' means of identification need to be crimes in themselves or should the law only criminalise the obtaining of a person's means of identification without their consent to commit other crimes?

I think that if the Iraqi legislature criminalises obtaining another person's means of identification without his consent, with intent to commit other crimes it will include even methods (such as phishing or spam) that may be used to obtain the means of identification. Therefore, it is unnecessary to criminalise these methods.

Q12. Do you think that the obtaining of another person's means of identification needs to be a crime in itself? Or should the law only criminalise other crimes that are committed subsequently (using another person's means of identification)?

I think that the obtaining of another person's means of identification should be a crime in itself. We cannot control crimes that are committed by using another person's identity unless we criminalise the obtaining of another person's means of identification or the tool that are used to this means of identification.