Cyberspace Identity Theft: An Overview

Nazura Abdul Manap

Anita Abdul Rahim

Hossein Taji

Faculty of Law, The National University of Malaysia (UKM), 43600 Bangi, Malaysia, Corresponding author: Hossein Taji
Email: h.taji359@gmail.com

Doi:10.5901/mjss.2015.v6n4s3p290

Abstract

The present age of technological advances have boosted the crime of cyberspace identity theft. Although this crime is not new, the Internet has expanded its scope and created innovative ways of committing it, leading to a new variant called cyberspace identity theft. The identity thief uses information relating to the identity of another person's such as name, address, telephone number, mother's maiden name, social security number, social insurance number, health card number, bank account information, driver's license number and date of birth. It is stealing someone's identity information to commit theft, fraud or other crimes. This paper aims to reviews the historical, international and regional background to the law relating to cyberspace identity theft. Also addressed, are the national, regional, and international approaches to combating the problem, with a particular focus on the United Kingdom, Malaysia and Iran.Given the above premise, one of the objectives of this chapter is to examine the meaning of cyberspace identity theft from a global perspective. It aims to advance an acceptable definition of cyberspace identity theft (in addition to other related concepts) such that it would be easy to identify the crime, facilitate its investigation, as well as prosecution.

Keywords: *cyberspace, identity theft, introduction, background*

1. Introduction

The advent of the Internet and computer technologies has had a significant influence on modern societies. Information can now be obtained with greater speed, and preserved on an unprecedented large scale. For most businesses, academic institutions, professions and governments, computers are indispensable to the discharge of everyday tasks.

However, those benefits come with challenges. New crimes have emerged, and existing ones exacerbated. (Clarke, 1998) Many countries now contend with incidents of cyberspace identity theft, cyberspace identity fraud, hacking, sabotage, electronic money laundering and child pornography, among others. (Cradduck, 2007) For example, websites, as well as online facilities such as emails and chat rooms, enable criminals to steal the personal information of innocent users, defraud them, and lauder the proceeds.

With the advent of the Internet, there has also been an increase in the numbers and forms of computer crimes, particularly cyberspace identity theft. This is because computers now possess telecommunication capabilities. Unlike previously when computer crimes were limited to incidents such as trespass, and the destruction of data, identity theft can now be perpetrated by re-routing web users from their intended destinations to bogus websites, unbeknown to them.

This paper provides background information on the history of cyberspace identity theft. The paper focuses on how cyberspace identity theft is perceived and tackled under existing legal regimes in three principal jurisdictions: the United Kingdom, Malaysia and Iran.

2. Background of Cyberspace Identity Theft

2.1 Historical Background of Cyberspace Identity Theft

Some commentators have likened cyberspace identity theft to a disaster that unfolds before one's eyes, something that continually grows and becomes more devastating. One can do nothing to stop it, and all the actions taken to head it off are in vain. While not being the same thing as an earthquake, hurricane, or tsunami, it is a phenomenon that causes the

same magnitude of damage to individuals, businesses and governments. (Schreft, 2007) Cyberspace identity theft has grown and evolved over the last 35 years to take on a relentless life of its own. According to reports, cyberspace identity theft is on the rise, since criminals have found how easy it is to transact fraudulent business activities by means of new technologies that are being introduced every day.

With the emergence of the Internet, the widespread use of credit cards, and the growing volume of e-commerce, the methods used for the commission of cyberspace identity theft changed dramatically. (Newman, 2005) Thieves turned to modern and sophisticated techniques, which enabled them to operate anywhere in the world, and to swindle thousands of people, without being detected. In other words, the Internet changed the traditional nature of identity theft in as much as the thieves are able to launch their attacks, and defraud a large number of people without having any physical contact with them.

There are significant differences between cyberspace identity theft, and that of the real world. One such difference is that, in the former case, the techniques are constantly evolving. This makes it difficult for law enforcement agencies to keep pace with them, and thus adopt appropriate investigation procedures. Furthermore, in comparison with its real world counterpart, cyberspace identity theft can inflict a greater deal of economic harm on victims. (Chawki, 2006) In the real world, two forms of threats typically confront a nation; internal and external. And separate social organisations exist to deal with each of them. Those organisations dealing with the traditional real world threats are evidently always indispensable. But the borderless nature of a cyber threat, such as cyberspace identity theft clearly highlights the necessity of revising the conventional nomenclature of internal and external threats.

An additional issue is that cyberspace identity theft can both facilitate, and be facilitated by other crimes. For example, identity theft may make possible crimes such as bank fraud, document fraud, or immigration offences, just as it may be aided by crimes such as theft in the form of robbery or burglary. This interrelationship between identity theft, and other crimes is a main problem in analysing trends in identity theft such as the offending, victimisation, or prosecution rates, and creates a policy issue that legislators may also wish to consider. (Finklea, 2012)

With the rise of the Internet and e-commerce, the personal information of a large number of people is readily available in the virtual world. Internet access is getting faster and cheaper, and more and more people from different parts of the world can use this modern technology, for business, or pleasure. As a result, cyberspace identity thieves are able to victimise many people from different parts of the world, stealing millions from individuals, businesses, and banks annually. Other bodies such as information brokers, medical, educational and government institutions may also be affected.

Cyberspace identity theft is not limited to financial losses. Victims may lose valuable credit records. This problem is exemplified by the case of *R v Harris*, (2004, B.C.J. No. 2847, BCPC 33, p. 532) where Harris was found in the possession of a notebook containing 39 Master Card accounts whose numbers belonged to his victims.

2.2 Background of International Law relating to Cyberspace Identity Theft

Cyberspace identify theft is now a major issue on the international scene. The arrival of the information technology revolution led to this scenario and spawned the birth of a host of non-traditional illegal activities. Unlike traditional crimes, they can be perpetrated without face-to-face interactions, behind the scenes and their spread is global. There are no international organisations that deal with such issues and that have developed specific cyberspace identity theft legislation to address them. Despite this, international and regional organisations have increased their activities in this area. For instance the Council of Europe's Convention on Cybercrime[1]is the first international treaty aimed at Internet and computer crimes through the harmonisation of the region's national laws, improving investigative techniques, and enhancing cooperation among European nations.

2.2.1 The Council of Europe's Convention on Cybercrime

The Council of Europe is an intergovernmental organisation, which has been in existence since 1949.[2] The Council of

[1] *The Council of Europe (CoE) and European Union (EU) are two distinct bodies established with the aim of enabling Europe and its member nations to prosper. The two organisations have their own sets of goals and objectives. Each of these bodies has its own subdivisions that specialise in various economic areas or uphold certain democratic concepts to ensure the utmost respect for human rights.*

[2] *Difference between European Union and Council of Europe, http://www.differencebetween.net/business/organizations-business/difference-between-the-european-union-and-council-of-europe. (03 September 2014).*

Europe had published a report in 1990, entitled, "Computer Related Crime",[3] which listed the minimum list of crimes that should be criminalised through legislative intervention, and a list consisting of offences where their criminalisation is optional. (Nilsson, 1989)

Since cyberspace is borderless, global norms and standards are needed in order to provide security against crimes in this virtual world. The Council of Europe's Convention on Cybercrime is a significant step in this direction. Signed in 2001 in Budapest, Hungary by the United States and 29 other countries, the principal aim of the Convention is the harmonisation of domestic substantive criminal law offences relating to cyberspace, as well as investigation procedures. (Chawki, 2006) It is the first multilateral instrument meant to foster the making of laws in order to curb the spread of crimes in cyberspace, and enhance efficiency in the investigation and prosecution of such crimes. "The Convention's drafters' principal concerns were two-fold. First, they wanted to ensure that the definitions were flexible enough to adapt to new crimes and methods of committing existing crimes as they evolve. Second, the drafters wanted the Convention to remain sensitive to the legal regimes of nation-states". (Jain, 2005)

As of October 2008, 45 states[4] had signed, while 23[5] had ratified[6]the Convention. The Convention has created substantive criminal law provisions that make it a criminal offence to have illegal access to computer systems or system interference, and is acknowledged to be a critical international instrument for combating cybercrime, with wide support from various international organisations.[7]

The Convention is made up of four main sections with their respective provisions and articles. The first section defines the various terms such as computer systems and computer data, and states that participating countries should take steps to prevent offences related to them such as cyberspace identity theft.

Procedural and investigation requirements and standards that have to be adhered to by member countries are outlined in the second section. The third section provides instructions to enable international cooperation through joint investigations of criminal offences, such as cyberspace identity theft, child pornography and fraud, as defined in section one. The final section covers measures relevant to the signing of the Convention, its territorial application, amendments, withdrawals, and federalism. (Chawki, 2006) Among the more important crimes covered by this Convention, which relate to cyberspace identity theft are:

Illegal access: Article 2 refers to not having the right to access a computer system by entering into a computer system or any part of it including the hardware components and data storage. It excludes the act of sending emails to a file system.

Illegal interception: Article 3 makes it illegal to intercept non-public transmissions of computer data without authorisation, whether by telephone, fax, email, or file transfers, and provides the right of privacy of data communications. (Hopkins, 2002) This covers interception through the use of electronic eavesdropping or tapping devices, although what constitutes lawful or unlawful forms of interception are not defined and left rather to individual national policies. (Chawki, 2006,p.30)

Data and system interference: Articles 4 and 5 criminalise the unauthorised destruction, deletion, deterioration, alteration, suppression of computer data or the hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or supporting computer data.

Misuse of devices: Article 6 relates to the use of certain devices for the commission of offences and includes

---

[3] Recommendation no 899 on computer related crime and final report of the European committee on crime problems, Strasbourg 1990.

[4] Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, the Former Yugoslav Republic of Macedonia, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, Norway, Poland, Portugal, Republic of Moldova, Romania, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Ukraine, the United Kingdom, the United States.

[5] Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, the Former Yugoslav Republic of Macedonia, France, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Slovakia, Slovenia, Ukraine, the United States.

[6] The need for ratification is laid down in Article 36 of the Convention.

[7] Interpol highlighted the importance of the Convention on Cybercrime in the Resolution of the sixth International Conference on Cyber Crime, Cairo: "That the Convention on Cyber Crime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cybercrime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages." http://www.interpol.com/Public/TechnologyCrime/ Conferences/6thIntConf/Resolution. asp (03 October 2014); The 2005 WSIS Tunis Agenda points out: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of infor- mation technologies" and regional initiatives including, but not limited to, the Council of Europe's Conventionon Cybercrime",http:// ec.europa.eu/ information_ society/activities/internationalrel/docs/wsis/tunis_agenda.pdf (03 October 2014).

tangible transfers as well as the creation or compilation of hyperlinks that facilitate access by hackers to them. (Chawki, 2006,p.31)

Article 8, segment 1 deals with computer related fraud: The Convention defines computer fraud as inputting, altering, deleting or suppressing computer data, or computer programs, or otherwise interfering with data processing which affects the result of data processing, and through this, causes economic loss or any seizure in the property of another person, in order to gain illegal economic interest for oneself or another person.[8] This definition supposes the integrity of the property, and considers possession as the primary legal interest, and security and transferability of money through data processing as the secondary one. The main objective is that any misuse in data processing for affecting the results, illegally transferring property, and causing damage is considered a crime. The targets of fraud are computer data and computer programs. The above definition covers all related misuses.

The Cybercrime Convention, in its preamble, similarly acknowledges that international cooperation is required in the fight against cybercrimes, including cyberspace identity theft. Chapter 3 of the Convention urges signatory countries to cooperate as much as possible through international agreements, treaties and domestic laws in the investigation of crimes and provision of evidence.[9] It also contains detailed provisions for mutual assistance in situations where there are no mutual assistance treaties.[10] No doubt, such a multilateral approach offers the best hope of coping with the ubiquitous nature of cyberspace identity theft.

In 2007, the Council of Europe published a study analysing various approaches aimed at criminalising Internet related cyberspace identity theft. The study noted that despite the provisions in the Convention no specific provision catered for cyberspace identity theft per se and that could be applied to all related acts. (Gercke, 2007)

2.2.2 The United Nations

The extent and seriousness of the problem of identity related crimes have also prompted the United Nations to take counter measures as part of its crime prevention agenda. The Bangkok Declaration on "Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice",[11] which was endorsed by General Assembly Resolution 60/177 of 16 December 2005, highlighted the criticality of tackling document and identity fraud towards checking organised crimes. Member States were urged, "to improve international cooperation, including through technical assistance, to combat document and identity fraud, in particular, the fraudulent use of travel documents, through improved security measures, and encourage the adoption of appropriate national legislation".[12]

In line with Economic and Social Council (ECOSOC) Resolution 2004/26, the United Nations Office on Drugs and Crime (UNODC) commissioned a study on fraud and the criminal misuse and falsification of identity. (UNODC, 2014) The study covered a wider scope than in the OECD[13] context in the following ways. First, the general term for identity related crime was broadened to include any form of illicit conduct involving cyberspace identity fraud and theft. Second, it also widened the scope in that the commission of all criminal activities whether on or offline were included with greater focus on sophisticated criminal schemes and patterns and their networks with transnational organised crime and other criminal activities. Finally, identity related crime was considered a part of fraud, given their nexus and in line with the ECOSOC mandate.[14] (Hand book on identity related crime, 2014)

Other UN resolutions also note the challenges related to cyberspace identity theft and the need for appropriate responses. This includes strengthening the United Nations crime prevention initiatives[15] that highlight cyberspace identity theft as a major policy issue, which should be explored by UNODC. Based on ECOSOC Resolutions 2004/26 and 2007/20, UNODC has established a group of experts to discuss the best course of action in this field.

---

[8] Council of Europe Convention on Cyber Crime 2001.
[9] Articles 23 and 25 of the Convention on Cybercrime.
[10] Article 27 of the Convention on Cybercrime.
[11] Bangkok Declaration, Synergies and Reponses: Strategic Alliance in Crime Prevention and Criminal Justice", 2005, endorsed by General Assembly resolution 60/177 of 16 December 2005, http://www.un.org/events/11thcongress/ declaration.htm (03 september 2014).
[12] Bangkok Declaration, Synergies and Reponses: Strategic Alliance in Crime Prevention and Criminal Justice, 2005, paragraph 27.
[13] On 14 December 1960, 20 countries originally signed the Convention on the Organisation for Economic Co-operation and Development.
[14] Hand book on identity related crime http://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html. (11 September 2014).
[15] United Nations General Assembly Resolution, Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity, A/RES/62/175, 2008, p 3.

2.2.3 Interpol

Interpol is an international criminal police organisation established in 1923 to facilitate cross border police cooperation even where diplomatic relations between countries do not exist and to support and assist all organisations, authorities and services involved in combating international crime. Its involvement in countering cybercrime capacity at the international level began very early. A survey of members on cyber criminal law in 1981 noted various issues related to the application of existing legislation in such criminal activities. (Schjolberg, 2007)Taking into account the legal gaps between countries and in the frameworks for countering such criminal activities, Interpol expanded its duties to include both law enforcement and harmonisation of the related legal provisions. (Xingan, 2007)

In its fight against international cybercrimes, Interpol includes financial and high-tech crimes such as unauthorised access, hacking, computer fraud and computer theft, which are relevant to cyberspace identity theft crimes.

2.3 Background of Regional Law relating to Cyberspace Identity Theft

Regional conventions attempt to provide a viable and legitimate basis for the fight against cyberspace identity theft. In this recognition, attempts have been made at the regional levels to grapple with the problem of cyberspace identity theft. At the regional level, the EU and the OECD have adopted similar initiatives.

2.3.1 The European Union

The European Union[16] has developed different legal instruments to handle identity related information such as the EU directive on privacy,[17] and the criminalisation of certain aspects of fraud and Internet related offences such as illegal access to computer systems.

The European Union is well aware of the challenges posed by such criminal activities and has taken policy level measures to combat them,[18] while the European Commission has proposed that EU law enforcement cooperation would be made more effective by criminalising cyberspace identity theft in all its Member States. This proposal opened the way for instituting consultation on whether specific legislation is necessary and appropriate in Member States in line with expectations of the public in Europe for their governments to prevent and punish the abuse of identity for criminal purposes. In mid-2007, the Commission (DG on Justice, Freedom and Security) authorised a comparative study on establishing a definition of cyberspace identity theft in Member States and their criminal consequences.

Most European countries possess two forms of anti-identity theft legislation namely the protection of privacy and protection against economic and financial crime. Although much effort was expended in the attempt to harmonise and unify data protection and privacy standards, differences prevail particularly in regard to the procedural and institutional framework. One noteworthy EU privacy legislation is the violation of substantive privacy rights and that related to formal legal requirements. Infringement of substantive privacy rights includes the following offences: the illegal entering, modification, or falsification of data with the intent to inflict harm or damage the storage of incorrect data. Such activities are covered by the general offences of information and by additional statutes within privacy laws. (Chawki, 2006,p.24)

The illegal disclosure, dissemination, obtaining of and/or access to data are activities covered in most laws though to varying degrees. With the rapid increase in computer related crimes globally countries feel the need for introducing new or stronger legislation to combat them. As already noted, among the legal instruments adopted to curb the problem of theft of identity is the Council of Europe's Budapest Convention on Cybercrimes, which marked a new paradigm of international cooperation in combating crime. Under the Convention, EU Member States and other signatories seek a

[16] *The Council of Europe (CoE) and European Union (EU) are two distinct bodies established with the aim of enabling Europe and its member nations to prosper. The two organisations have their own sets of goals and objectives. Each of these bodies has its own subdivisions that specialise in various economic areas or uphold certain democratic concepts to ensure the utmost respect for human rights.*

[17] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

[18] *As part of an awareness campaign to improve the prevention of identity theft and payment fraud, Directorate- General Justice, Freedom and Security (DG JLS) and Directorate-General Internal Market of the European Commission organised a conference on "Maintaining the integrity of identities and payments: Two challenges for fraud prevention", which took place on 22–23 November 2006 in Brussels. The Conference intended to emphasise the importance of the wider involvement of policy makers and high ranking representatives of national administrations and to provide a plat- form for policy makers to discuss possible EU initiatives in this field. Among the issues discussed at the Conference were possible EU criminal legislation on identity theft, training models for law enforcement/financial investigators, exchange of information and privacy issues.*

supranational regulatory framework for that purpose by facilitating its detection, investigation and prosecution domestically and internationally. (Chawki, 2006,p.24)

2.3.2 The Organisation for Economic Cooperation and Development (OECD[19])

In 1983, the OECD established an expert committee to discuss the computer crime phenomenon and criminal law reform. The OECD defines computer and computer related crime as illegal, unethical, or unauthorised behaviour involving automatic data processing and/or transmission of data. Among the committee's recommendations in its 1985 report is that, owing to the particular nature of cybercrime, international cooperation is vital to reduce and control such activities and recommended that member countries amend their penal legislation to cover cybercrime. (Shalhoub, 2010) A guideline was proposed for such purposes and a list of offences made to enable standardised policies and legislation to address computer related crimes such as computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorised access, unauthorised interception, unauthorised reproduction of a protected computer program and unauthorised reproduction of topography. (Global Cyber Law, 2014)

In 1999, the OECD Council approved a set of guidelines designed to protect electronic commerce that included developing strategies to prevent cyberspace identity theft. However, they do not contain approaches to criminalise specific aspects of such theft. In 2003, the OECD developed another set of guidelines related to cross border fraud but these too do not explicitly deal with how to criminalise cyberspace identity theft, but enable the development of a broader framework to investigate and prosecute such offences. In 2008, the OECD published a "Scoping Paper on Online Identity Theft" (OECD, 2008) that provided a detailed analysis of different Internet related cyberspace identity theft scams that also covered victims and law enforcement schemes. In the same year, it published the "Policy Guidance on Online Identity Theft" (OECD, 2008)which provided an outline of appropriate strategies to combat such theft on the Internet.

Much of the OECD's emphasis in this context is on educating and raising awareness of consumers, businesses, government officials, and the media on cyberspace identity theft to prevent them from falling victim as well as to facilitate government efforts to combat such criminal activities. The mode of operation, incidences and types of computer crime is disseminated and consumers made aware of cyberspace identity theft and how it is perpetrated through techniques, such as pharming, smishing, and vishing. (OECD, 2008) The role of the government to combat cyberspace identity theft is paramount and a common definition for it in the policies and strategies of different countries will make a big difference. This is especially since different countries view it differently with some treating it as a crime and others as a preparatory step towards other wrongs. This is a major reason why even the legislation on it differs in different countries. (Stickley, 2009)

These various definitions show the inability to arrive at a consensus on what constitutes cyberspace identity theft. (Gercke, 2007) This has to be addressed to enable the drafting of clear-cut and unambiguous criminal law provisions.

The broadness of the terms 'identity theft' and 'identity fraud' make their treatment different. As such, the use of the term 'identity crime' to cover both was suggested by the United Nations Intergovernmental Expert Group when working on Fraud and the Criminal Misuse and Falsification of Identity in 2007. However, this itself, poses another problem, as in some countries these offenses are as yet not considered crimes.

Another difference is that most of the definitions stress on the act of obtaining information, which limits the scope in drafting criminal law provisions to issues of data espionage. (Gercke, 2007) As different definitions lead to different laws, cyberspace identity theft is associated with fraud while others focus on how the stolen information is used to commit crimes. What is common is that they have the offences criminalised whether the information is stolen or when it is used.

2.4 Relevant Laws relating to Cyberspace Identity Theft in the United Kingdom

The United Kingdom law relating to cyberspace identity theft is influenced by the Convention on Cybercrime, being a signatory thereto. The key piece of legislation dealing specifically with computer crimes is the Computer Misuse Act 1990. Under Section 1 of the Act, it is a crime to obtain data without authorisation through the use of a computer. The impact of this provision is to make it an offence to use identity theft techniques, such as spyware, Trojan horse, and hacking. (CIPPIC, 2007) However, a technique such as phishing, or other social engineering techniques through which victims are tricked into volunteering their personal information, are not covered, since such information is not accessed without authorisation. (CIPPIC, 2007) Moreover, under Section 2 of the Act, unauthorised access with intent to commit or

[19] On 14 December 1960, 20 countries originally signed the Convention on the Organisation for Economic Co-operation and Development.

facilitate the commission of further offences constitutes a crime. This section is a useful net for catching offences that are perpetrated through electronic means such as those pertaining to theft and fraud.

Another law relevant to cyberspace identity theft in the United Kingdom is the Data Protection Act 1998, which protects personal data. The Act covers all personal data, which an organisation may hold, including names, birthday and anniversary dates, addresses, and telephone numbers. It regulates what information may be collected by data holding organisations, as well as the uses to which they may be put. Under Section 55 of the Act, it is an offence to unlawfully obtain personal data from a data holding organisation. This provision also makes it an offence to sell or offer personal data for sale. Under the section, merely advertising personal data will amount to offering such data for sale. Pursuant to the same section, acts such as hacking, and the use of spyware, or social engineering techniques to obtain personal data is an offence. Section 13 of the Act provides remedies for victims whose identity has been stolen because of the failure of data holding organisations to comply with the Act. There is, however, no provision in the Act requiring the notification of security breaches, a lacuna that could lead to personal information being undermined. (CIPPIC, 2007)

The Criminal Justice Act 2003 of the United Kingdom is equally relevant to cyberspace identity theft. Under Section 3, it is an arrestable offence to provide a false statement for the purposes of obtaining a passport. Moreover, Section 286 thereof tightens the penalty imposed for fraudulently obtaining a driving licence. In addition to these laws, the United Kingdom also has the Identity Cards Act 2006. Under Section 25 of the Act, it is an offence to possess false identity documents, or identity documents relating to other persons. However, in order to constitute an offence, the possession of such documents must be with the intent of using or inducing other persons to use them to "establish a registrable fact". The said section further makes it an offence to possess any device designed to make false documents, or any material used to make such documents.

2.5 Relevant Laws relating to Cyberspace Identity Theft in Malaysia

Malaysia has introduced a number of new laws in recognition of the need for new legislation in order to tackle the problem of computer crimes. A major piece of legislation in this regard is the Computer Crimes Act of 1997 (CCA). The CCA creates three main offences, which relate to the misuse of computers: unauthorised access to computer material, unauthorised access with intent to commit other offences, and unauthorised modification of computer contents. The CCA is aimed principally at overcoming the shortcomings of traditional laws. For example, the offence of unauthorised access does not require the element of moveable property, or corporeal property, which does not suit the nature of digital crimes. (Nazura Abdul Manap, 2012)

Under Section 4 of the CCA 1997 an offence aimed at committing fraud, dishonesty or to cause injury as defined in the Penal Code, or that facilitates such offences whether by himself or another person attracts a fine not exceeding 150,000 ringgit or to imprisonment for a term not exceeding 10 years, or both. (Section 4 Computer Crime Act 1997)Such offences under this section are classified as unauthorised access and the act of committing or facilitating those three activities.

This section examines the efficacy of the Computer Crime Act 1997 in handling crime, which cannot be done via the traditional laws. Cyberspace identity fraud is covered under Sections 4 of the CCA 1997 that specifically covers crimes committed through computers and/or computer systems which facilitate their commission such as through the creation of fake credit cards, credit card fraud or by online banking fraud.

In cyberspace identity fraud, the offender employs false statements and misrepresentations to induce a victim to relinquish property voluntarily. This is a common form of criminal act committed through the Internet under schemes such as multilevel marketing or pyramid networks, business opportunities or franchises, auctions, general merchandise sales, credit card offers, advance fee loans and employment offers. The Internet facilitates the perpetration of such deceptive activities as it enables easy communication with victims via e-mails, websites or social networks. (Nazura Abdul Manap, 2012)

Section 5 of the CCA 1997 deals with criminalising unauthorised modification of computer content programmes or data and imposes a punishment on perpetrators whether the intent existed to make the modification aimed at those activities.

Wrongful communication is addressed under section 6 where a person is guilty of an offence if he uses in a computer whether directly or indirectly a number, code, or password which he is not authorised to communicate, the wrongful commission of which attracts a maximum fine of 25,000 ringgit or seven years imprisonment or both.

The CCA 1997 also contains provisions intended to facilitate the investigation of crimes, and the general enforcement of the Act. Under the Act, there is a rebuttable presumption that a person who has in his custody or control, program, data, or other information held in a computer or retrieved from a computer, and which he is not authorised to

have in his custody or control, has obtained unauthorised access to same. The most significant aspect of the CCA 1997 relating to the cyberspace idenity theft cases is found in Section 9, which makes the Act applicable extraterritorially. The CCA 1997 applies inside as well as outside Malaysia, whatever the nationality or citizenship of the persons involved, and any offence committed under the Act outside Malaysia may be treated as having been committed within Malaysia. In addition, the CCA 1997 will apply if the computer, data or program was in Malaysia, or capable of being connected to, sent to, used by, or with a computer in Malaysia at the material time of the commission of the offence.

With regard to search and seizure powers, in cyberspace identity theft cases, pursuant to Section 10 of the CCA 1997, when a Magistrate has a reasonable cause to believe that there is evidence of the commission of an offence under the Act, he may, by warrant, grant a police Inspector the power to search for, seize and detain any such evidence. In addition, any police officer may arrest, without a warrant, any person whom he reasonably believes to have committed, or to be committing an offence prohibited under the Act. Any person obstructing, or delaying the police in the discharge of their duties under the Act is also guilty of an offence.

While the CCA attempts to cover all computer related offences, a key question is whether it is adequate? Given the evolving nature of these offences, there seems to be a need to constantly review the Act if it is to deal effectively with such offences. Furthermore, unlike the laws of other countries, which not only punish offenders, but also provide compensation to victims, the CCA 1997 does not provide any form of compensation to victims.

2.6 Relevant Laws relating to Cyberspace Identity Theft in Iran

The first proposal for a Computer Crimes Act was made in the Iranian Parliament on 19 November 2008, with 176 votes in favour, 3 against, and 2 recusants. After its approval by the Supreme Council of Cultural Revolution, and the Islamic Parliament, as well as its confirmation by the Guardian Council, it was finally enacted into law on 29 June 2009. The Act has 5 parts and 55 sections. It provides for two types of punishment, namely a jail term, fine, or both of them. (Dezyani, 2007)

Article 1 of the CCA 2009 (Article 729 of the Islamic Penal Code 1970) covers the crime of unauthorised access, and its procedures are similar to that applied under the Convention of Cyber Crime 2001. Unauthorised access is considered the primary and most prominent computer crime under this article as it leads to other illegal acts such as cyberspace identity theft that is aimed at stealing information and data. The penalty for being found guilty of committing unauthorised access to computer (telecommunication) systems or data protected by security measures is 91 days to one year of imprisonment or a fine of between 5 million to 20 million rials, or both.

Article 2 of the CCA 2009 (Article 730 Islamic Penal Code 1970) states that unlawful access to any protected system is prohibited and paragraph B provides a general definition of unauthorised access. Unauthorised access by persons is aimed at committing other unlawful acts. Under this paragraph, the penalty for selling, distributing or exposing passwords or any other data that enables unauthorised access to computer or telecommunication data or systems owned by others is 91 days to 1 year's imprisonment or a fine of 5 million to 20 million rials, or both. Therefore, even knowing and using another person's password to enter a system is considered unauthorised access is committed as it enables personal data to be stolen.

Article 12 of the CCA 2009 (Article 740 of the Islamic Penal Code 1970) states that "whoever robs data belonging to another person in an unauthorised manner, if the exact data were in the hands of their owner, would be condemned to a fine in cash from one million to twenty million Rials, and otherwise would be condemned to imprisonment from 91 days to one year, or fine in cash from five million to twenty million Rials, or both of them".

Article 13 of the CCA 2009 (Article 741 of the Islamic Penal Code 1970) relates to computer fraud where anyone in any manner interferes with any normal action of a computer or related systems that infringes on their social and employment rights and responsibilities, or secures monetary gain or profit through such an action is guilty of fraud and liable imprisonment of one to five years and a financial penalty equivalent to the amount of gained by their fraudulent action.

With regard to the jurisdiction on cyberspace identity theft cases Article 28 Computer Crime Act 2009 (Article 756 of the Islamic Penal Code 1970) provides that Iranian courts are competent to deal with cases involving:

i. Confidential data, or the data used in committing a crime, in any way saved in computer and telecommunication terminals, or data carriers within the scope of Iranian land, sea, and air space;
ii. Crimes committed through websites whose domains are in Iranian code;
iii. Crimes committed by any Iranian or non-Iranian out of Iranian territory against Iranian computer and telecommunication systems, websites under the control of the three branches of government (legislature, executive, and judiciary), the Iranian leadership institution, official governmental agencies, any agency or

institution offering public services, or against the websites whose domains are in Iranian code in an extensive level; and

iv. Crimes involving the abuse of under-aged persons (persons below the age of 18), whether the offender or victim be Iranian or non-Iranian.

As can be seen, cyberspace identity theft is now receiving attention in Iran. Until 2009, there was no law for computer crimes, in general, and cyberspace identity theft, in particular. Pre-existing laws only catered to the classical types of theft. However, Iranian legislators have now adopted new regulations dealing specifically with cyberspace identity theft in order to provide security in the virtual world.

3. Elements In Interpretation

There is still no globally recognisable definition for identity theft committed in cyberspace or even in the physical world. (Cops, 2009) There remains considerable relativism in the way different countries perceive this phenomenon. Some conflate both forms of theft, and make no distinction between them. Some others do not even view it as a crime.

Nonetheless, mindful of the continuing difficulty in arriving at a commonly accepted definition, cyberspace identity theft may be defined as the unauthorised collection, transfer, retention or use of information relating to a natural or a juridical person for the purposes of perpetrating further crimes such as theft, fraud and other similar crimes through computer systems and networks. (Cradduck, 2007, p.140) Thus, it is two-stage crime: first, is the unauthorised collection of personal information relating to other parties, and second, is the fraudulent use of such information to secure a benefit to the detriment of the owners. (CIPPIC, 2007) Therefore, in this paper, the term will be considered to refer broadly to the collection and fraudulent use of information belonging to another person. It includes the unauthorised collection of another person's information, as well as the forgery of identity documents, and the fraudulent use of such information.

3.1 Unauthorised Collection of Information

Cyberspace identity theft begins with the collection of personal information belonging to other people, living or dead, without their knowledge and permission, usually through deception, and which information is used immediately, transferred to another party, or preserved for the commission of other crimes at a later date. Such information helps cyberspace identity thieves to perpetrate other crimes, which may involve taking over a victim's financial account, renting apartments, or enjoying the services of utility companies, all in the victim's name. (CIPPIC, 2007)

3.2 Fraudulent Use

Usually, cyberspace identify thieves indulge in the unauthorised collection of other peoples' personal information with the motive of putting such information into fraudulent use in order to achieve some economic benefit, such as access to credit cards and loans, leaving the victims to face the consequences. (Nahaludin Ahmad, 2009) This means that cyberspace identity theft involves impersonation. Identity thieves hide under the identities of their victims in order to commit different crimes by using the names, addresses, birth certificates, passports, insurance, telephone, or identification numbers, as well as credit card and bank account details of those victims. (Nahaludin Ahmad, 2009) This fraudulent use of information may be repeated over time, without the knowledge of the victims, leading to accumulated losses. It is clear, therefore, that cyberspace identity theft entails both the unauthorised collection of personal information belonging to other parties and the subsequent use of that information in a fraudulent manner. (CIPPIC, 2007) It comprises numerous aspects, and forms just a part of a broader web of crimes carried out at different stages.

4. Conclusion

Recent technological advances have boosted the crime of cyberspace identity theft. Although this crime is not new, the Internet has expanded its scope and created innovative ways of committing it, leading to a new variant called cyberspace identity theft. Identity thieves no longer need to search waste bins or come into personal contact with victims in order to steal their personal information for fraudulent uses. In spite of these changes, there is still no widely accepted definition for cyberspace identity theft. Without doubt, a clear and acceptable definition is crucial to combating cyberspace identity theft in terms of criminalising, investigating, prosecuting, and punishing it, as well as differentiating it from other crimes. However, most of the existing definitions suffer from ambiguity or lack of completeness. There are also stark differences in definition among countries, with some viewing cyberspace identity theft as a crime and others, as a civil wrong. Moreover, the definitions focus unduly on the act of obtaining information, further restricting the scope of many penal provisions to data collection. In this recognition, attempts have been made at the national, regional and international

levels to grapple with the problem. At the national level, efforts have been made by countries such as the United Kingdom, Malaysia and Iran through the enactment of new pieces of legislation and the revision of old ones. At the regional level, the EU and the OECD have adopted similar initiatives. Notable at the international level are the efforts of the Council of Europe through the Convention on Cybercrime, the UN, as well as Interpol. An additional difficulty is the confusion between 'identity theft' and 'identity fraud', with the UN Intergovernmental Expert Group suggesting that the term 'identity crime' be used instead to cover both. As indicated earlier, such a suggestion is equally problematic because cyberspace identity theft is not yet perceived as a crime in some countries. These variations in perspectives have led to correspondingly contrasting policies and laws. The differences in definition highlight the difficulty faced in trying to reach an agreement on what cyberspace identity theft really is. The resulting variations in legal perspectives, in turn, present obstacles to collective attempts to combat the problem. Therefore, a clear and widely accepted definition of cyberspace identity theft is needed in order to enact equally unequivocal laws.

5. Acknowledgment

This article is an output to the Universiti Kebangsaan Malaysia's research grant of Geran Galakan Penyelidikan Industri 2013 (Industri-2013-037).

References

A. Jain, (2005). *Cyber crime Issues Threats and Management*, India, Chawla Offset Publication.

Canadian Internet Policy and Public Interest Clinic, Australian, French, and United Kingdom legislation relevant to identity theft: an annotated review, CIPPIC Working Paper No. 3C (ID Theft Series), March 2007, p 3.

G. R. Newman, (2005). *Identity Theft Literature Review*, the U.S. Department of Justice, 210459, p 13-18.

Global Cyber Law Database, International Development of Cyber Law,http:/ /www.cyberlawdb.com/main/international-development (04 September 2014)

Hans. G. Nilsson, (1989). The council of Europea fights computer crimes, *Computer Law & Practice*, 6 (18). http://www.unafei.or. p/english/pdf/RS_No65/No65_07VE_Nilsson2.pdf (22 October 2014)

Hand book on identity related crime http://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html. (11 September 2014).

H.Cops et al, (2009). Understanding identity theft offenders accounts of their lives and crimes, 3 (34), *Criminal Justice Review*, p 330.

http://www.rooznamehrasmi.ir.(03 September 2013)

http://www.majlis.ir (05 October 2013).

http://www.iran bar.ir/. (08January 2014).

K. M. Finklea, (2012). Identity Theft: Trends and Issues, CRS Report for Congress Prepared for Members and Committees of Congress, R40599, p 23.

L. Xingan, (2007) International actions against cybercrime: Networking legal systems in the networked crime scene'. http://www. webology.org/2007/v4n3/a45.html (28 September 2014).

L. Cradduck et al, (2007). Identifying the identity thief: Is it time for a (smart) Australian card? 16(2) *International Journal of Law and Information Technology,* p 140.

M. Chawki et al, (2006). Identity theft in cyberspace: Issues and solutions, 11(1) *Lex Electronica*, p 7.

M. H. Dezyani, (2007). Computer Crime, *Informatics*, p 28.

M. Gercke, (2007). *Internet Related Identity Theft*, Project on Cybercrime, Council of Europe, p 15.

N.Abdul Manap, (2012). Cybercrimes: Problems and solutions under Malaysian Law, 2 *'lawyer',* Khorasan Bar Association, p151.

N. Ahmad, (2009). Truth about identity fraud: Defence and safeguards, 9 *Current Law Journal*, p 13.

OECD, (2008). Scoping Paper on Online Identity Theft, Ministerial Background Report.DSTI/CP, 3/ FINAL, OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June, p 12.

R. Clarke, (1998). Information privacy on the Internet: Cyberspace invades personal space, 48 (2) *Telecommunications Journal of Australia,* p 4.

S. L. Schreft, (2007). Risks of identity theft: Can the market protect the payment system? 92 (4) *Economic Review - Federal Reserve Bank of Kansas City,* p 20.

S. L. Hopkins, (2002). Convention on cybercrime: A positive beginning to a long road ehead, 2 (1) *Journal of High Technology Law*, Suffolk University School of Law, p 105.

Stickley. Jim, (2009). *The Truth about Ideutity Theft*, New Jeresey, Pearson Education Inc, p 2.

S. Schjolberg et al, (2007). *Computer Related Offences*, Conference on the Challenge of Cybercrime, Council of Europe, Strasbourg, France, , http:/ /cybercrimelaw .net /documents/strasbourg.pdf (04 September 2014).

UNODC,response,to,identity,related,crime.http://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html. (11 September 2014).

Z. K. Shalhoub, (2010). *Cyber Law and Cyber Security in Developing and Emergine Economies*, United Kingdom, Edward Elgae Publishing, p 2.