Cyberspace Identity Theft: The Conceptual Framework

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.v6n4s3p595

Abstract

The present age of technological advances has extended the reach of crimes into the Internet. Nevertheless, while the Internet may have led to the emergence of wholly new crimes, it has mostly brought about new ways of committing preexisting crimes. (Garner, 2000) For example, although it is often called a 21st century phenomenon, (Hoar, 2001) cyberspace identity theft is, in fact, not a new type of crime. (United Nations, Handbook on Identity Related Crime, 2011)Long before the emergence of the Internet, identity thieves stole people's identities through dumpster diving by searching for personal identifying information such as social security and bank account numbers in the trash left outside people's homes. 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.

Keywords: *cyberspace, identity theft, terminology, types, techniques*

1. Introduction

The advent of the Internet has changed trend dramatically by introducing a new variant called cyberspace identity theft. (OECD Policy Guidance on Online Identity Theft, 2008) This is a technology-based form of identity theft, which is perpetrated through the medium of the Internet. It involves stealing someone's personal information such as name, date of birth, address, social security number, social insurance number, health card number, bank account information, driver's licence number, and the like, for the purposes of committing a theft, fraud or other crimes. (Chawki, 2006)

For example in the case of *R v McNeil,* (2006, B.C.J. NO. 187, BCPC, p. 32) the accused possessed a variety of personal information belonging to his victims, including driver's licence, health card, home address, home phone number, cell phone number, date of birth, bank and line of credit balances. A similar situation occurred in the case of *Bongeli v Citibank Canada,* (2004, 7 O.J. No. 3272, p. 132) where the thief, Bongeli, was found in the possession of personal information belonging to a number of individuals. Clearly, with the increasingly global tendency towards the digitisation of human affairs, (Gercke, 2012) it is now possible for fraudsters to carry out their criminal activities through the Internet.

Thus, the Internet has made it easier for identity thieves to steal the identifying information of innocent victims for use in fraudulent activities, since transactions can now be concluded without any need for personal interaction. Criminals no longer have to snatch wallets from victims in order to obtain their money, or personal particulars that may be contained in them. Instead, they steal the online personal information of such victims, which allows them to access their bank accounts, or commit other online crimes using the stolen information. (Beigelman, 2009)

An equally worrisome fact is that while the physical methods of stealing a person's identifying information are well known, this is less so for cyberspace identity theft techniques, such as phishing, pharming, smiShing, vishing, fake job advertisment, hacking, preying on social networking sites, and use of malware. (CIPPIC, 2007) This invites a need to foster appropriate awareness about the latter.

Given the above premise, one of the objectives of this paper 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.

Another task this paper undertakes is an examination of the various types of cyberspace identity theft, and the relevant techniques used in committing them. The final section concludes the paper.

2. The Definition of Key Terminologies

Cyberspace identity theft is a new phenomenon arising from the creation and advancement of technology. Like other offences it needs to be clearly defined to allow for proper monitoring, investigation and prosecution especially since the elements of crime inherent in it are reflective of other cyber crimes. Unfortunately, there is no current single universally acceptable definition for cyberspace identity theft. This situation needs to be addressed to enable appropriate mechanisms to be put in place so as to ensure that the rights and properties of people are safeguarded, and the investigations and prosecution of violations are facilitated.

This part of the paper examines the issue of identity theft on cyberspace, with due reference to the various definitions and classifications in existing journals, reports, statutes and judicial cases. It strives for a suitable definition of cyberspace identity theft, and begins by considering the definition of 'cyber' and 'cyberspace', as well as 'identity', 'theft' and 'identity theft'. The discussion is mainly based on the dictionary, technical and legal definitions, which attempt to look at the terminologies from different perspectives.

2.1 Cyber and Cyberspace

Since this paper is relates to the legal issues raised by identity theft on cyberspace, it is important to define cyberspace.

2.1.1 Dictionary definition

2.1.1.1 Cyber

Cyber is a new phenomenon associated with the Knowledge Age. The Advanced American Dictionary, Longman, defines it as "a prefix relating to computers". For example, a cybercafe means a cafe equipped with computers connected to the Internet for customers' use, and cyberphobia is an irrational fear of computers. Cyber is also defined in Technodictionary.com as "a prefix taken from the word, "cybernetics" (the Greek word, *kybernan*, which means to steer, or govern), and attached to other words having to do with computers and communication". Based on these definitions, it may be said that cyber is a non-physical world, which is the brainchild of computer systems.

2.1.1.2 Cyberspace

According to the Longman dictionary, 'cyberspace' or 'cyberia' is a term used in computer science, which signifies, "all the connections between computers in different places, considered as a real place where information, messages, pictures etc. exist". Webopedia defines it as, "a metaphor for describing the non-physical terrain created by computer systems". As this online dictionary explains, "online systems, for example, create a cyberspace in which people can communicate with one another (via e-mail), do research, or simply window shop". It continues by noting that, "like physical space, cyberspace contains objects (files, mail messages, graphics, etc.), and different modes of transportation and delivery".

2.1.2 Technical definition

2.1.2.1 Cyber

According to Technodictionary.com, the term, 'cyber' was coined from the word 'cybernetics', which has its origin in the Greek word, *kybernan* (meaning to steer or govern), and used in combination with other words relating to computers and communication. This means that the term is used as prefix for capturing humans, things or ideas connected to recent developments in computer and information technologies. Webopedia similarly defines 'cyber' as one of the increasing number of terminologies used to describe new products created as a result of the availability and use of computers. The key features that cut across these definitions are interconnected information systems and the human users that interact with them. The human factor is the most significant feature of cyber, it being a human creature. This point is apparently reflected in the 2001 Congressional Research Services (CRS) Report for the U.S. Congress, which in this respect referred to the total inter connectedness of human beings. (Schaap, 2009) In the same respect, Graham Todd more specifically refers to, "an evolving man-made domain". (Graham Todd, 2009)

2.1.2.2 Cyberspace

The origin of the term, 'cyberspace' can be traced to a work of fiction authored by William Gibson. He described cyberspace as, "a graphic representation of data abstracted from banks of every computer in the human system". (Gibson, 1984) 'Cyberspace' is defined in Webopedia as, "a metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery". A notable characteristic of cyberspace is that people do not have to move physically from one point to another within it in order to perform their activities. They can carry out such activities far away, without moving physically from their location, simply by clicking a mouse or punching a key on a computer keyboard.

Attempts to define cyberspace were also made by Reheingold and Cavoukian. Rheingold asserts that cyberspace is, "the conceptual space where words, human relationship, data, wealth and power are manifested by people using CMC (computer mediated communications) technology". For Cavoukian, the term means, "the electronic airways and information residing in electronic or digital form, capable of being transmitted online via networked communications". (Cavoukian, 1997)

From the above definitions, it can be summarised that cyberspace is all about a space having a digitised form, where all its activities, data and contents are transmitted and actualised through a 'networked communication' technology. This is why the term 'Internet' and 'cyberspace' are almost always interchangeably used.

2.1.3 Legal definition

2.1.3.1 Cyberspace

Numerous definitions have been proffered for cyberspace. Providing a clear definition is indispensable to any meaningful analysis of the term. Legally speaking, cyberspace, and real space are not the same. (Cohen, 2007) Therefore, both must be differentiated, and treated separately. (Folsom, 2007) Attributing the rules of real space to cyberspace does no good, and may lead to legal conflicts. (Folsom, 2007) This is because offences committed in cyberspace vary from those carried out in the real world; the former are committed at an alarming rate, and their repercussions, unlike those of the real world, are comparable to weapons of mass destruction. (Folsom, 2007) Furthermore, cyber criminals do not need costly, organised secret plans in order to execute their schemes. Simply clicking a mouse will suffice. The cost of committing a cybercrime is low, indeed. This is because the crime can be executed on a computer by causing it to perform a criminal activity on another computer system, for example, through data manipulation, or disruption. (Cohen, 2007)

2.2 Identity, Theft and Cyberspace Identity Theft

Defining cyberspace identity theft has equally proven to be a problematic task. Numerous definitions have been proffered. Still, no globally acceptable definition exists, whether for cyberspace identity theft, or its real world variant. Perhaps, in defining cyberspace identity theft, it is proper to begin by examining the notions of identity (personal information) and theft.

2.2.1 Dictionary definition

2.2.1.1 Identity

The term, 'identity' is defined in the Oxford English Dictionary as "the set of behavioural or personal characteristics by which an individual is recognised". (Weiner, Oxford English Dictionary, 1991) In the Merriam Webster online dictionary, 'identity' is defined as, "who someone is: the name of a person. The qualities, beliefs, etc., that make a particular person or group different from others". It is a collection of defining attributes that differentiates one individual from another.

2.2.1.2 Theft

The term, 'theft' is defined in the Oxford English Dictionary as, "the action or crime of stealing". (Weiner, Oxford English

Dictionary, 1991)In the Merriam Webster online dictionary, 'theft' is defined as, "a: the act of stealing; specifically the felonious taking and removing of personal property with intent to deprive the rightful owner of it; b: an unlawful taking (as by embezzlement or burglary) of property".

2.2.1.3 Identity theft

Online British dictionary defines the 'identity theft' as "the crime of setting up using bank account and credit facilities fraudulently in another person's name without his or her knowledge". In the online reference dictionary, 'identity theft' is define as, "the fraudulent appropriation and use of someone's identifying or personal data or documents, as a credit card". In the Merriam Webster online dictionary, 'identity theft' is defined as "the illegal use of someone else's personal identifying information (such as social security number) in order to get money or credit".

2.2.2 Technical definition

2.2.2.1 Identity theft

Traditionally, identity reminded us of a person's name. Now, however, the scope of this term has been broadened to include bank, credit card and social security numbers. With the advances in technology, identity may now also cover PIN numbers, computer usernames, passwords, email addresses, fingerprints, iris and DNA.

The UK Home Office Report on Identity Fraud offers three categories of identity. (Britz , 2007) One is attributed identity. This covers those attributes assigned to an individual usually upon birth, such as names, date, and place of birth. (Koops, 2009) The second is biometric identity, which are attributes peculiar to an individual, such as fingerprint, iris, and DNA profile. (Koops, 2009) The third, which is biographical identity, refers to those attributes that an individual has accumulated in his life time, including academic and professional credentials, work history, birth and marriage registration, among others. (Britz , 2007) This covers both the dictionary and the technical definitions considered earlier.

As is clear from above, some identifying attributes are acquired at birth, while others are issued by government, or private bodies. Thus, identity may also include a person's social security number, bank account number, credit card number, PIN number, username and password, as well as e-mail address. (OECD , 2007) Cyberspace identity theft will normally involve attributed identity and biographical identity.

2.2.3 Legal definition

With regard to theft, it includes, "the felonious taking and carrying away of the property of another". (Nahaludin Ahmad, 2009) This definition raises, at least, two questions. First, is whether personal information qualifies as 'property'. Second, is whether personal information is amenable to 'taking and carrying away'. Under Section 4 (1) of the English Theft Act 1968, for example, property encompasses "money and all other property, real or personal, including things in action and other incorporeal property". While this definition is, to a certain extent, a tautology (for example, it says that property includes "all other property"), it, does, at least, suggest that personal information may qualify as property. This is because it provides that property may also include "things in action and other incorporeal property".

Nevertheless, it has been held that the English Theft Act 1968 does not properly cover intangibles, such as confidential information and trade secrets. In *Oxford v Moss*, (1989, 68 Cr. App. Rep, p.183) the accused, who had obtained a proof copy of examination questions, was charged with the theft of information belonging to his university. The prosecution argued that the information was property capable of being stolen because it entailed a proprietary right of confidence. The breach of that confidence, therefore, amounted to the theft of the information. However, the defence counter argued that, under Section 4 of the Theft Act, intangible property did not cover information. The presiding magistrate agreed with the defence, and held that confidential information did not qualify as property under Section 4 of the Act. His Honour stressed that confidence was not property in itself, but only a right over property, which conferred the right to control the dissemination of the proof.

On appeal, the Divisional Court similarly took the view that the definition of 'intangible property' under Section 4 of the Act was not sufficiently broad as to cover confidential information. The Court referred to other cases dealing with trade secrets and matrimonial secrets, and concluded that those cases related to confidentiality, the breach of which was remediable by way of injunction, or damages, rather than criminal sanctions.

It is true that theft has traditionally been used in relation to physical property. (Cradduck, 2007) For example, Section 378 of the Penal Code of Malaysia provides that "whoever, intending to take dishonestly any movable property

out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft". The section then lists examples of actions that could constitute theft, all of which involve tangible items.

According to Article 197 of the Islamic Penal Code 1970 of Iran also the essential element of theft in Iranian law is 'property'. Therefore, those things, which are not property according to law, and are not ownable, could not be the subject of theft. Here, it is disputable whether a 'property', which is the subject of theft, should be tangible or not.

However, the idea that identity cannot be stolen has been challenged. This is because in the digital era, identity can be embedded in mere information that is widely accessible, rather than in "flesh". (Caslon Analytics, 2013) Additionally, identity theft does restrict the ability of victims to use their identities since they may be denied credit, will be unable to operate new financial accounts, rent accommodation, or obtain driving licences. (Dadisho, 2005) Thus, it is argued that a party who assumes another person's identity without the latter's consent, does not merely borrow, or copy that identity, but steals it. (Cradduck, 2007)

Moreover, in the House of Lords case of *Rank Film Distributors Ltd. v Video Information Centre*, (1981, 2 W.L.R, p. 380) the respondent, who was facing a copyright infringement claim, resisted the appellant's discovery efforts because the disclosure of the documents sought would have exposed them to criminal prosecution for the theft of copyright interests, thereby undermining their privilege against self-incrimination. This implies that copyright, being an incorporeal thing is considered as property. Such a contention enjoys additional support from the UK Copyright, Designs and Patent Act 1998, which provides that copyright "is a property right". Analogically then, personal information, even though incorporeal, qualifies as property too.

But even if personal information is considered to be property, the next question is whether it meets the notion of 'taking and carrying away, and can, therefore, be the subject of theft. On one view, unless personal information is stored in a device, which is removed, it is unlikely to meet the condition of 'taking and carrying away'. (Nahaludin Ahmad, 2009) But it should be pointed out that in *Grant v* Allan, (1987, SCCR, p. 402) it was agreed that 'take' could entail causing a computer to make printouts, rather than the removal of already generated printouts. Despite that, however, the notion of 'taking and carrying away' seems unhelpful, because personal information, even if not stored in a device, is still amenable to theft.

For example, under the English Theft Act 1968 mentioned previously, a person who dishonestly appropriates another person's property with the intention of permanently depriving him of it, is guilty of theft. This means that the misappropriation of another person's information (property) can amount to theft. There is no requirement of 'taking and carrying away'. (Section 378 Penal Code of Malaysia) However, there is an additional requirement; an intention to permanently deprive the owner of the information. It has been argued that this requirement may not be met in the case of personal information in cyberspace identity theft. (Nahaludin Ahmad, 2009) This is because the misappropriation of a person's information may not necessarily be accompanied by the intention to permanently deprive him of that property. Nonetheless, a potential counter argument, according to one analysis, is that, while not permanently depriving the owner of his personal information, the misappropriation does, at least, deprive him of the exclusive possession of it. However, such an argument, if countenanced, it has been argued, would have relevance only in relation to confidential information, as in the case of trade secrets, where a case of theft may be made. (Watson, 2007)

Since a trade secret may consist of intangible information, and still be amenable to theft, there is, arguably, no reason why personal information cannot be stolen because of its intangibility. Furthermore, with the recent advances in computer technologies, information stored in a computer device could be copied (theft) on a grand scale at considerable speed, without the need to remove the storage device temporarily, or permanently. (Nahaludin Ahmad, 2009) Not surprisingly, in a jurisdiction such as the U.S., information is capable of forming the subject matter of theft. In *United States v Girard and Lambart,* (2011, 440 Fed. Appx, p. 894) the Court of Appeal for the Second Circuit considered the abstraction and sale of information, without permission, as falling under a law that prohibited the sale, without permission, of any 'record or thing of value'.

2.3 Finding an appropriate definition for cyberspace identity theft

As pointed out earlier in this paper, there is still no globally recognisable definition for identity theft committed in cyberspace or even in the physical world. (Cops, 2009) 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) Thus, it is a two-stage crime: first, the unauthorised collection of personal information relating to other parties, and second, 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.

2.3.1 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. (CIPPIC, 2007) 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)

2.3.2 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.

Under the two broad categories mentioned above, several more specific types of cyberspace identity theft can be identified. The more important of these are discussed below.

3. Types of Cyberspace Identity Theft

Cyberspace identity theft is not a stand-alone crime; it leads to the perpetration of other crimes. The Identity Theft Resource Center, which advises governmental agencies, educates the public and supports consumers, as well as identity theft victims, points out that such theft is not limited to financial crimes. The Center, which also provides advisory services to legislators, laws enforcement agencies and businesses, classifies cyberspace identity theft into six categories. The following is some of the most common types of cyberspace identity theft.

3.1 Financial Identity Theft

This involves using another person's information to obtain some benefits, such as goods, services, and credit, or to access a bank account. (Gercke, 2007) It may take one of two forms; true name identity, or account takeover. (Gercke, 2007) In the former case, the thief uses the stolen personal information to open a new credit card account that gives him access to credit, or a checking account that enables him to obtain blank cheques in the victim's name. In the latter case, the thief accesses accounts already opened by the victim by using the stolen personal information of that victim.

3.2 Medical Identity Theft

In medical identity theft, the perpetrator, without the victim's knowledge and permission, uses latter's name, often in addition to other items of information relating, for example,to insurance, to secure medical benefits involving goods, or services, or to falsely secure reimbursements for medical goods, or services purportedly enjoyed. (Stroup, 2013) The perpetrator's action may lead to the distortion of the victim's medical record with potentially fatal consequences when wrongful medical decisions are taken concerning the victim.

3.3 Criminal Identity Theft

In this case, the criminal falsely claims to be the victim when apprehended by the police for a crime. The criminal's claimed identity may be based on identity papers actually issued by the government, but which have been applied for and obtained, using credentials stolen from the victim. The result is that the criminal's real identity is concealed, and charges may eventually be brought against the victim, instead of the criminal. (Benner, 2000) The victim may only get to know what has happened when summoned to court to answer criminal charges arising from the perpetrator's action.

In such theft cases, victims are often unaware that crimes have been committed in their names and that they are likely to be held responsible for any criminal activity commited in their names. A victim may only be aware of what had transpired when he is summoned for a court appearance, applying for driving licence renewal, stopped by the police for a traffic infraction, or when finding that his license has been suspended or has been blacklisted. Job opportunities may also be lost because of a fraudulent criminal act.

3.4 Synthetic Identity Theft

This may involve the partial or full fabrication of an identity. For example, a real social security number may be combined with a name, and birth date that are different from those of the real owner of the social security number. (Gercke, 2007) It is more challenging to trace crimes committed with the aid of this form of identity theft. This is because they are usually not reflected directly in the victim's record such as his credit report. Instead, they may emerge as brand new files, or as an auxiliary part of the victim's existing credit report. The loss from this form of identity theft is normally borne by creditors who mistakenly extend credit to the criminal. But the individual victim may also be imperilled because the synthetic identity may ultimately be mistaken for his name, or the negative entries in his auxiliary credit report may result in unfavourable credit ratings.

3.5 Identity Cloning and Concealment

The perpetrator in this case impersonates another person with a view to keeping their real identity discreet. In some cases, the perpetrator's aim may simply be to maintain anonymity on personal grounds, (Koops, 2009) although the usual motive is to commit a crime. Identity cloning and concealment may never be uncovered, especially in those cases where the perpetrator has successfully acquired false documents that enable him to scale through routine authentication tests. (CIPPIC, 2007) This contrasts with financial identity theft that may ultimately come to light when huge debts have been accumulated in the victim's name. (Benner, 2000)

In such cases it is not the financial or medical gain that the information thief seeks, rather it is aimed at obtaining employment or even using the victim's name in all settings. Such thieves are usually convicted criminals on the run from the law, illegal immigrants, or those seeking to hide their identities and establish new ones for personal and psychological reasons. Identity cloning is facilitated by social networking sites as they request users to disclose personal information.

3.6 Child Identity Theft

In this kind of identity theft, the criminal, often a person who typically preys on children, or a relative, (Stroup, 2013) uses a child's social security number to obtain some benefit, such as access to credit. Owing to the fact that the social security numbers of minors carry no information, they are particularly useful to identity thieves. One study found that as many as 10.2% of 40,000 children surveyed were victims of identity theft. (Richard, 2013) As minors, the victims of this kind of identity theft may only discover what is happening much later in their lives, meaning that the crime can continue for a long period of time. (Stroup, 2013)

The above analysis shows the different forms that cyberspace identity theft may take. Two main categories were identified. One is true name identity theft. In this case, the thieves steal the personal information of their victims, which is fraudulently used to obtain financial, medical and other benefits, by impersonating the victims. The other is account takeover identity theft, which involves the taking over of existing accounts belonging to victims. This is normally carried out by intercepting victims' correspondence relating to financial transactions by unlawfully changing their addresses to those of the thieves. Within these general categories, there exist numerous types of cyberspace identity theft. Some of the major ones include criminal identity theft, financial identity theft, medical identity theft, and synthetic identity theft. Others are identity cloning and concealment and child identity theft.

Understanding the multiplicity of ways in which cyberspace identity theft occurs provides insights into the real

problems that individuals, businesses, governments, and law enforcement authorities face, in addition to potential pathways for tackling its occurrence. Problems relate not only to financial losses, but also the medical risks to which innocent victims are exposed due to distortion in their medical records. In addition, victims may be charged and convicted for offences they did not commit, or denied employment and credit facilities, unless they clear their names, usually after protracted ordeal and expenses.

The analysis also demonstrates that it is quite a challenging task to detect some types of cyberspace identity theft, especially synthetic identity theft and identity cloning and concealment. In the former, for example, the crime does not appear directly on existing victims' records, such as credit reports, but in new files, or as auxiliaries to those credit reports. This makes it harder for law enforcement authorities to detect the crime, the effect of which would, in many cases, be borne by creditors that have mistakenly granted credit to the thieves.

Worse still, in some cases, as in identity cloning and concealment, the crime may never be discovered, particularly if the thieves are able to obtain fake documents that make it possible for them to pass through routine security checks successfully. Another glaring fact is that children are equally vulnerable to cyberspace identity theft. The fact that the social security numbers of children typically bear no data, makes them good targets for cyberspace identity thieves. The result is that children may be confronted later in life with criminal records they know nothing about.

Finally, it should be noted that cyberspace identity theft is not a stand-alone crime. It is simply the starting point of many other types of crimes. Thus, it may involve several stages, perpetrated at different times and places, as well as through different techniques. This complexity increases the difficulty encountered not only in trying to conceptualise the phenomenon, but also to curb it. As this paper has attempted to do, it is necessary to decompose cyberspace identity theft into its different composite elements, including the techniques used to perpetrate them in order to attain a better grasp of the concept. Accordingly, the next section of this paper examines some of the techniques employed by cyberspace identity thieves.

4. Techniques of Cyberspace Identity Theft

An appreciation of the techniques used in the commission of identity theft in cyberspace is vital to our understanding of the crime, and possible modes of prevention. (OCED, 2008) This makes it pertinent to examine some of the more common of those techniques.

4.1 Phishing

Through this technique, criminals impersonate legitimate organisations and send out fake text messages, emails (spoofing), or phone calls in the names of those organisations with the intention of luring victims into disclosing personal information. (Jakobson, 2013) For example, the criminals may set up a fake website in the name of an established travel agency, and deceive unsuspecting victims to reveal their credit card details in order to buy tickets. Based on the existing literature, phishing is the most prevalent cyberspace identity theft technique, having proven successful in many cases. (Jakobson, 2013)

4.2 Pharming, SmiShing, Vishing

4.2.1 Pharming

As discussed in paragraph 4.1, pharming, or domain spoofing, is derived from the term phishing, and involves the use of a spoofed website to lure unwitting individuals into giving their personal information. It can be accomplished in two ways. In the first technique, the computer host's file is compromised by entries, which send legitimate domain names to illegitimate IP addresses. The second technique, known as Domain Name System (DNS) poisoning, exploits weaknesses in DNS software to gain control over the domain name of an existing website and the numeric address changed. Consequently, when Internet users enter the affected website address, they will automatically be directed to the spoofed site, even though their browser's address bar will retain the original correct address and thus deceived into believing that the site is legitimate. (CIPPIC, 2007)

4.2.2 Smishing

Under smishing, cell phone users receive text messages from a company confirming their signing up of one of its dating

services for which they will be charged a certain amount per day unless the order is cancelled at the company's website. Such a website is in fact compromised and used to steal personal information. (Stroup, 2014)

4.2.3 Vishing

In a classic spoofed e-mail, appearing from legitimate businesses or institutions, the phisher invites recipients to call a telephone number, which requests personal data such as account number, or password for apparent security verification purposes. Victims usually feel this is safe as they are not required to go to a website to transmit that information. (Stroup, 2013)

4.3 Abuse of Privileged Access

In this case, the personnel of government and credit institutions who have privileged access to databases containing personal information may collude with strangers and make the information available to them. Often, the identity thief may be an employee, for example, of a bank, who uses customers' personal information, such as social security numbers, addresses and account details to open credit accounts.

4.4 Hacking

Identity thieves may also break into computer systems, networks, and databases in order to extract large amounts of personal information. (Ealy, 2013) Hacking involves the unlawful access to a computer system (Australian Institute of Criminology, 2005) and is among the oldest computer related crimes, which has become a serious and widespread phenomenon. Apart from famous targets like NASA, the United States Air Force, the Pentagon, Yahoo, Google and eBay, (CIPPIC, 2007) offenders increasingly target the computer systems of regular users to obtain identity related information or aim for systems that host large databases for the same purpose.

4.5 Fake Job Advertisements

Another identity theft technique is the issuance of fake job advertisements. (CIPPIC, 2007) In this way, identity thieves deceive victims into submitting resumes containing their personal information such as full names, qualifications, phone numbers, email addresses, and account numbers.

4.6 Use of Malware

The use of malware is an additional form of identity theft technique. By using malware such as keystroke logging programs, or other forms of spyware, such as Zeus, identity thieves (Giles, 2010) attack communications between users and their computers in order to obtain personal information. Malware may also be used to attack communications between a user's computer system and the Internet, or to interfere with Wi-Fi signals. (OCED, 2008) Through this means, emails may be diverted and personal information, such as bank, and credit card statements intercepted. In some cases, trojan horses may be used to hijack web browsers, making it possible to intercept information entered by users, who may also be redirected to bogus websites for the same purpose by means of spoofing. Apart from individual users, identity thieves may also use malware to attack communications between service providers and other entities with which they maintain business links, such as banks. (CIPPIC, 2007)

4.7 Preying on Social Networking Sites

A popular identity theft technique is the infiltration of a social networking site, such as Facebook in order to collect personal information disclosed by users. Such information, including poorly protected downloadable photographs, is then used to impersonate users with increased credibility. (Gercke, 2007) In some cases, identity thieves pretentiously befriend users only to trick them into revealing their personal information such as bank account numbers, credit card numbers, and home addresses. (Biegelman , 2009) Based on the information so obtained, identity thieves may successfully infer additional users' information, such as social security numbers. (CIPPIC, 2007)

From the foregoing analysis, it can be seen that various techniques and modes of operations are used by criminals to gain access to the personal information of others. These methods increasingly reflect a higher level of sophistication

and expertise and criminals have various motives for doing so, but primarily seek to obtain some financial gain and to conceal their wrongdoings.

The degree of sophistication of the techniques vary considerably with some being extremely elaborate, especially those used over the Internet, which require intimate and expert knowledge of computer technology. Techniques involve deceiving unsuspecting and trusting information custodians into releasing personal information or hacking to gain access to that information. Alternatively, identity theft can be as simple as sifting through the garbage of an organisation or an individual to find discarded documents containing valuable personal information.

A major characteristic of cyberspace identity theft techniques is the high degree of anonymity it affords criminals, thereby making it an extremely popular mode of operation as well as providing very lucrative returns to them.

New techniques and modus operandi are constantly being discovered by identity thieves, and as committing theft in the traditional way becomes more difficult and less profitable, it is expected that criminals will resort to new forms of cyberspace identity theft. This creates further exposure for individuals and a real challenge for law enforcement officials and legislators. (CIPPIC, 2007)

5. Conclusion

As a fast growing social issue, cyberspace identity theft is drawing the attention of the public, media and governments. Although it is not a new crime, a new variant of it has emerged with the advent of the Internet. It is considered to be an exciting issue not just in terms of the number of cases, but also in the amount of suffered.

The first glaring issue in cyberspace identity theft, is the absence of a clear definition. This issue has also been identified as one of the major obstacles to the conduct of scientific research, and the interpretation of findings. Moreover, without a clear definition, it will be difficult to formulate effective laws to tackle the crime. It is not possible to tackle what cannot be defined. Only with a clear definition will it be possible to spell out in any proposed legislation the elements that constitute the crime. Due to this factor, a commonly agreed definition of cyberspace identity theft remains lacking.

Moreover, the issues in the definition of cyberspace identity theft are too complicated. Due to the fact that cyberspace identity theft can be carried out anywhere in the world, it has blurred national boundaries. Therefore, provisions that are limited to a particular region will hardly be efficient. In fact, most countries do not provide legislation that is cyberspace identity theft specific. Consequently, they may have to rely on other related pieces of legislation in order to cover the elements involved in cyberspace identity theft offences.

It is hard to arrive at a generally accepted definition for cyberspace identity theft. However, the crime may be said to involve a number of activities which include, at least, the unlawful collection, possession, or transfer of another person's information, with or without the intention of using it to carry out fraudulent or other criminal activities.

There exist numerous types of cyberspace identity theft. Some of the major ones include criminal identity theft, financial identity theft, medical identity theft, and synthetic identity theft. Others are identity cloning and concealment and child identity theft. The analysis demonstrates that it is quite a challenging task to detect some types of cyberspace identity theft, especially synthetic identity theft and identity cloning and concealment.

Cyberspace identity thieves take advantage of different methods such as phishing, pharming, smiShing, vishing, fake job advertisment, hacking, preying on social networking sites and use of malware in order to gain access to people's identifying information. But, cyberspace identity theft is not an end in itself. Instead, it is a preparatory step towards the commission of other crimes. There are various uses of cyberspace identity theft. Most commonly, it is used in perpetrating other criminal acts. For example, an identity thief may present a victim's personal identifier when apprehended by the police. (CIPPIC, 2007) He may also use a victim's personal information such as a social security number in applying for credit cards, loans, goods, homes, medical and utility services. (Nahaludin Ahmad, 2009) A cyberspace identity thief could, in addition, use a victim's personal information to open new bank accounts, take over existing ones, or divert to his own address, sensitive financial correspondence meant for the victim, by applying for change of address. (Chawki, 2006) Moreover, cyberspace identity theft may be used to compromise medical insurance, and credit card payment systems. Other uses of cyberspace identity theft include terrorism and unauthorised immigration. However, cyberspace identity theft is not always used for criminal purposes. Sometimes, it may be motivated simply by the quest for fun or fame. (Ramage, 2005)

6. 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. Cavoukian. Tapscott, (1997). *Who knows: Safeguarding your privacy in a networked world*, New Yourk, McGraw Hill Publication, p 51.

Australian Institute of Criminology, (2005). http://www.aic.gov.au/publications/htcb /htcb005.pdf (03 September 2014).

B. Koops et al, (2009). A typology of identity related crime: Conceptual, technical, and legal issues, 12 (1) *Information, Communication & Society*, p 3.

Canadian Internet Policy and Public Interest Clinic, (2007). *Techniques of Identity Theft*, CIPPIC Working Paper No.2 (ID Theft Series), p 15.

E. Dadisho, (2005). *Identity theft and the police response: Prevention, The Police Chief the professionalvo ice of law enforcment*. www.policechiefmagazine.org. (3 May 2013).

G.H.Todd, (2009). Armed attack in cyberspace**:** Deterring asymmetric warfare with an asymmetric definition, 65, *The Air Force Law Review*,http://lexisnexis.com. (25 September 2014).

Hoar, (2001). Identity theft: The crime of the new millennium, 80 (1), *Oregon Law Review*, P 14-21.

J.E.Cohen, (2007). Cyberspace As/And space, 210, *The Columbia Law Review*, http://www.lexisnexis.com (25 September 2014).

J. Stroup, The Basics of Medical Identity Theft Can It Even Be Fixed?, http//idtheftabout.com/od/recoveringyouridentity/a/Medical_IDT_General.htm (3 May 2013).

J. Benner et al, (2000). Nowhere to turn: Victims speak out on identity theft, A CALP IRG/Privacy Right Clearinghouse Report, http://www.privacyrights.org/ar/idtheft2000.htm (25 April 2013).

J. Giles, (2010). Cybercrime made easy, 205 (2) *New Scientist,* p 20-21.

Korea Communication Commission, (2008). OECD Policy Guidance on Online Identity Theft, OECD Publication, p 2.

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 130.

M. Chawki et al, (2006). Identity theft in cyberspace: Issues and solutions, 11(1) *Lex Electronica*, p 5.

M. Gercke, (2012).*Understanding Cybercrime: Phenomena, Challenges and Legal Response*, Switzerland, ITU Publication, P 1. http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html(7 Apr 2013).

M. T. Beigelman, (2009). *Identity Theft Handbook: Detection, Prevention and Security*, 1st Edn, New Jersey, United States of America, John Wiley & Sons Publication, p 4.

M. Schaap, (2009). Cyber Warfare Operations: Development and Use Under International Law, *The Air Force Law Review*. http://www.afjag.af.mil/shared/media/document/AFD-091026-024.pdf (25 September 2014).

M.T. Britz, (2007). *Computer Forensics and Cyber Crime*, 2nd Edn, Paris, OECD Publication, p 119.

M. Gercke, (2007). Internet Related Identity Theft, Project on Cybercrime, Council of Europe, 22 November, p 16.

M.T.Biegelman, (2009). *Identity Theft Handbook: Detection, Prevention, and Security*, 1st Edn, Wiley Publication, United States of America, p 6.

N. Ahmad, (2009). Truth about identity fraud: Defence and safeguards, 9, *Current Law Journal*, p 2.

R. Garner, (2000). An overview of computer related crime, 7 (1) *Telemasp Bulletin,* p1.http://ww w.lemitonline.org/publications/telemasp/Pdf/volume%207/vol7no1.pdf (7 Apr 2013).

T. C. Folsom, (2007). Defining cyberspace (Finding Real Virtue in the Place of Virtual Reality)75, (9) *Tulane Journal of Technology and Intellectual Property*, http://www.lexisnexis.com(25 September 2014).

United Nations, (2011). *Handbook on Identity Related Crime*, New York, United Nations Publication, P 28.

W. Gibson, (1984). *Neuromancer,* New York, Ace Books Publication, p 50-55.