The Construction of Identity Offences Taxonomy: An Australian Context

Lesley Land
Security eCommerce Assurance Research Group
UNSW Business School
University of New South Wales
Kensington, New South Wales
Email: L.Land@unsw.edu.au

Stephen Smith
Department of Computing
Faculty of Science
Macquarie University
North Ryde, New South Wales
Email: Stephen.Smith@mq.edu.au

Donald Winchester, and
Vincent Pang
UNSW Business School
University of New South Wales
Kensington, New South Wales
Email: D.Winchester@unsw.edu.au,
Vincent.Pang@unsw.edu.au

Abstract

The objective of this project is to create an identity crimes taxonomy as a foundation for highlighting the importance of a National Identity Security Strategy (NISS 2012) initiated by the Commonwealth of Australia. The purpose of the taxonomy is to ensure that there is a common reference point for identity (related) crimes in the future for all the Commonwealth, State and Territory Government agencies. That is, the same identity definitions can be applied consistently across all Government agencies. This, in turn, will facilitate the measurements of the different identity (related) crime classifications across Australia, and therefore, enable the design of a holistic strategy for implementing solutions for managing identity crimes in Australia. Our challenge is to ensure that the taxonomy build for the Commonwealth of Australia can also be applied in the academic research. The taxonomy is constructed from a modified Nickerson et al. (2013)'s taxonomy development methodology.

Keywords (5 words)

Identity, Identity Crime, Identity Fraud, Identity Theft, Identity Offences Taxonomy

INTRODUCTION

The 2010-11 Personal Fraud Survey conducted by Australian Bureau of Statistics (2012) estimated A$1.4 billion was lost due to identity offences. The National Identity Security Strategy (NISS) initiated by the Commonwealth of Australia with the support of State and Territory governments, was purposely developed to address identity security measures that help to prevent, deter, detect and measure identity offences (NISS 2012).

The objective of this project has been to create a taxonomy for identity crimes and identity related crimes/misuses as a foundation for implementing the NISS. The purpose of the Identity Offences taxonomy is to ensure that there is a common reference point for identity offences for all the Commonwealth, State and Territory Government agencies. The need for a reference point is at least twofold. Firstly, as we observe that information systems are being increasingly used in a variety of ways to combat and support crime management, the need for a taxonomy becomes crucial for consistent storage and retrieval of identity crimes data across different agencies and institutions. Secondly, over time, historical data based on a common framework of reference can be meaningfully used to carve out operational, tactical and strategic approaches to deal with identity crimes. Without an agreed upon taxonomy, different government agencies will be relying on their own definitions and frameworks, and hence consolidated analyses, costings, approaches, and strategies are virtually impossible in the face of limited resources.

The pervasiveness of computers and the Internet has resulted in many identity offences (such as credit card fraud and romance fraud) being committed via the Internet. In addition, technologies (such as credit card skimmers) have been used to facilitate identity offences, such as creating fake credit cards, or skimming credit card details.

In this paper, an Identity Crimes Taxonomy is constructed to specifically depict identity offences and other related criminal activities. The aim of this paper is to construct the Identity Offences taxonomy based on multiple sources including: (A) government reports obtained from the Committee of the Standing Committee of Attorneys-General of the Commonwealth, State and Territory Governments in Australia (e.g. MCLOC 2008); (B) academic literature (e.g. Jamieson et al. 2008, 2012); (C) comprehensive literature review concerning existing taxonomies; and (D) data and feedback from government agencies. Amongst others, an important outcome of the Identity Crimes Taxonomy is to highlight how identity offences could impact on governments, businesses and individuals. In turn, the developed taxonomy could be used as the basis to identify and measure identity offences so that programs and policies can be designed and implemented to combat identity crimes.

For rest of this paper, we explain how the taxonomy is constructed. We recognise the linkages that identity crime is closely associated with other types of prevalent crimes such as cybercrimes. We also address the limitations of the proposed taxonomy and propose a structure of grouping Identity Crimes consistently.

LITERATURE REVIEW

Crimes involving the theft or impersonating using false identities has probably been enacted since the dawn of civilization. ICT is being used to for criminal activities on an ever increasing scale with greater sophistication and from international locations. While most Identity crimes use false credentials and can be easily classified as common fraud. The execution of the associated crimes like deception, money extortion (in romance fraud cases) create deliberation whether these class of crimes can be considered specific to identity crime cases of whether they should be prosecuted under existing laws (MCLOC 2008; Mitchell et al. 2013). In Australia, the Commonwealth and state jurisdictions have offences that specifically prohibit the possession and use of false identities. However, most cases of identity crime appear to be prosecuted under general laws, thus masking the ability to collect and classify any statistics relating to identity crime cases (Johns, 2012). Models and conceptual frameworks for identity fraud are emerging and have been developed broadly on themes that have investigated costs (Cuganesan and Lacey 2003; Newman and McNally 2005), profiling (Le Lievre and Jamieson 2005), processes (Jamieson et al. 2007) and definitions (MCLOC 2008; Sproule and Archer 2007; Wang et al. 2004).

Traditionally the background of identity crimes was largely documented under the umbrellas of security and privacy (Straub, 1990). However there is still a paucity of literature on identity crimes. They are sometimes referred to by other terms such as "*identity fraud, identity theft and identity deception or false identity, assumed identity, fictitious identity, identity fabrication, synthetic identity fraud, manipulated identity, counterfeit identity and impersonation fraud*" (Jamieson et al., 2008).

Recent literature – white papers, academic papers, government reports and websites – acknowledge that there are no universal standard definitions for identity terms such as identity crime, identity theft and identity fraud (Finklea 2014). Most papers explain definitions of key terms either from dictionaries or government papers (see ACPR and AUSTRAC 2006). Jamieson et al. (2008, 2012) also reviewed the literature and attempted to find a common ground for the identity definitions. In this paper, we further extend their work by searching and collecting identity definitions across the agency websites published by the Australian Commonwealth, State and Territory Governments. We also found that the definitions from these sources were widely applied or paraphrased across the Government agencies. Given these precedents, these definitions would serve as an appropriate foundation for constructing the taxonomy. These definitions were also compared with definitions which we proposed in our previous publications, and other academic publications.

Our literature review found that most of the government websites make references to a few online sources (websites and publications) for further information on identity crimes. In other words, the key terms have not been rigorously analysed. Also, even across all the Australian government agencies, identity terms have not been consistently defined. Thus the definitions they publish can refer to different types of identity offences. Differences and nuances in definitions suggest the large variations, conditions, and combinations in which crimes can be committed. Without an agreed taxonomy and associated definitions, a fraudulent activity could be classified and prosecuted differently.

METHODOLOGY

We adopt a methodology from our previous paper (Land et al. 2013), which, in turn, was based on Nickerson et al. (2013) Taxonomy Development Methodology. As shown in Figure 1, the work on this paper follows the Empirical-to-Conceptual path, indicated as a thick red line. In other words, this taxonomy was mainly developed from literature, case studies and feedback from the stakeholders.

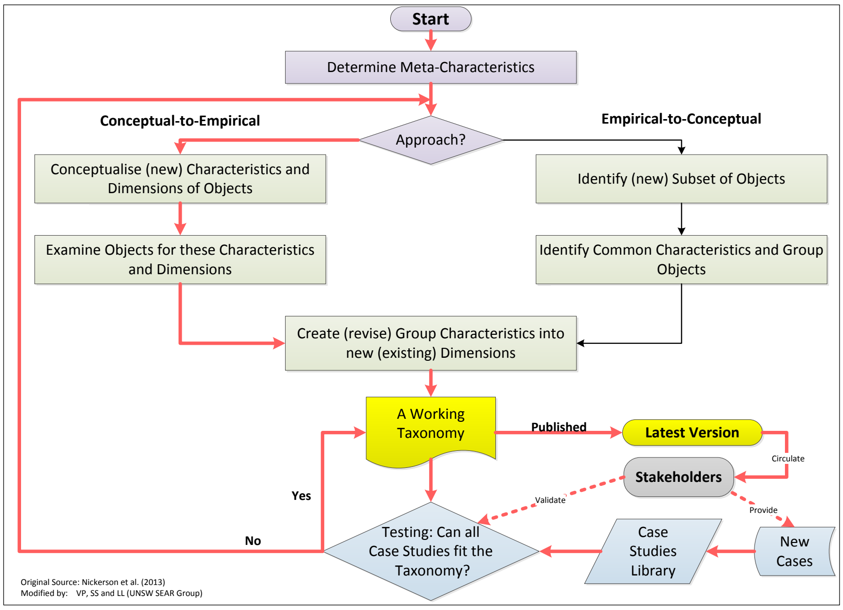
Start
Determine Meta-Characteristics
Conceptual-to-Empirical
Empirical-to-Conceptual
Approach?
Conceptualise (new) Characteristics and Dimensions of Objects
Identify (new) Subset of Objects
Examine Objects for these Characteristics and Dimensions
Identify Common Characteristics and Group Objects
Create (revise) Group Characteristics into new (existing) Dimensions
A Working Taxonomy
Published
Latest Version
Circulate
Stakeholders
Validate
Provide
Yes
No
Testing: Can all Case Studies fit the Taxonomy?
Case Studies Library
New Cases
Original Source: Nickerson et al. (2013)
Modified by: VP, SS and LL (UNSW SEAR Group)

Figure 1: Taxonomy Methodology (Land et al. 2013)

We used identity offence case studies from published Government documents to validate the taxonomy. The taxonomy was circulated among the stakeholders, and received feedbacks over time from them. We then modified the taxonomy to address the feedbacks. The taxonomy went through several iterations. Although the taxonomy is purposely constructed for the Commonwealth of Australia, we believe this taxonomy can also be used as a reference point in the academic research.

IDENTITY OFFENCE TAXONOMY

We first present our Identity Offence Taxonomy as shown in Figure 2. Next, we define the identity terms, follows by justifying the terms used in constructing the taxonomy.

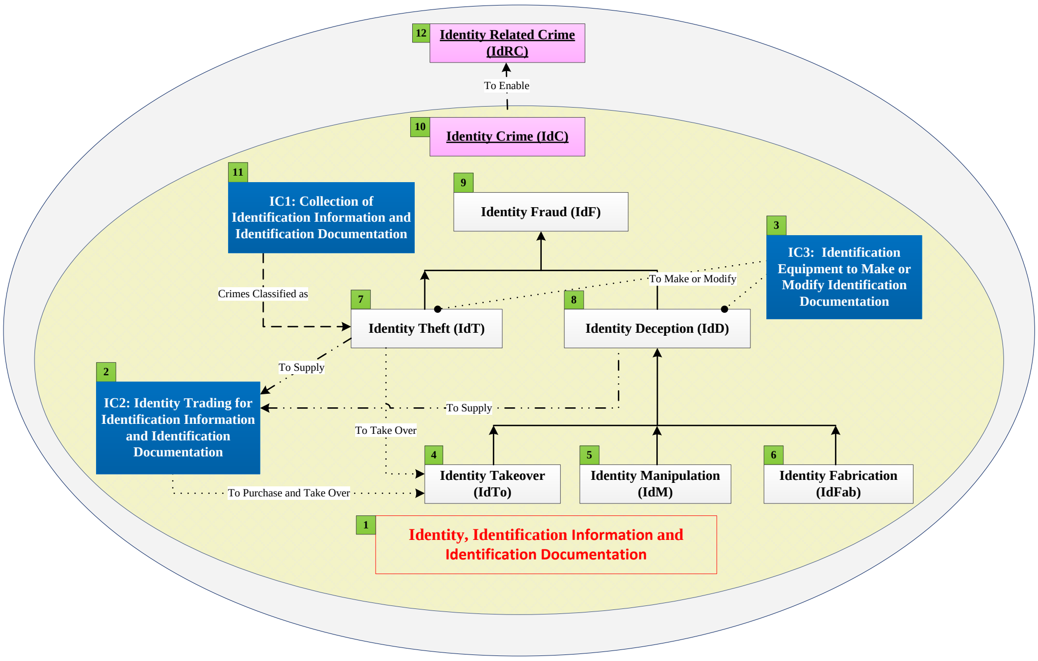
12
Identity Related Crime (IdRC)
To Enable
10
Identity Crime (IdC)
11
IC1: Collection of Identification Information and Identification Documentation
9
Identity Fraud (IdF)
3
IC3: Identification Equipment to Make or Modify Identification Documentation
To Make or Modify
Crimes Classified as
7
Identity Theft (IdT)
8
Identity Deception (IdD)
To Supply
2
IC2: Identity Trading for Identification Information and Identification Documentation
To Supply
To Take Over
4
Identity Takeover (IdTo)
5
Identity Manipulation (IdM)
6
Identity Fabrication (IdFab)
To Purchase and Take Over
1
Identity, Identification Information and Identification Documentation

Figure 2: Identity Offences Taxonomy

Naming of Identity Offences Taxonomy

Before discussing how the terms used in taxonomy, we first justify the naming of the taxonomy. Many identity terms such as identity crime, identity theft, identity fraud, and identity crime offence have been used to describe a crime related to the compromise of an identity. Instead, we borrow a general term *identity offence* from the New South Wales legislation (Johns 2012) to label crimes that are related to the compromise of an identity, which basically encompasses all the above identity terms. In the New South Wales legislation, the identity offence is formulated with variations based on Model Criminal Law Officers Committee (MCLOC 2008).

Identity Definitions used in Taxonomy

Instead of reinventing the identity definitions, we first choose to use the existing published definitions to begin with. The selection of definition sources was based on suitability of the descriptions for the taxonomy. We only introduce or redefine a definition when necessary. For instance, we add “digital identifiers” to the identity definition (See No 1 in Table 1) as today’s smartphones is part of our lives as we use smartphones, for instance, not only for phoning and texting but using the apps such as Facebook, Skype and What’s Apps for online communication, and banking and payment for goods and services. Thus, we will have a number of user ids and password for each of the applications and services. The numbering and definitions in Figure 2 are listed in Table 1. The reference column in the table is an indicator if we have created (‘New’) or modified (‘Modified’) the definition. The numbers reference the identity terms are from Figure 2.

Table 1 - Summary of Identity Definitions (as stated in Figure 2)

No	Identification Definition	Description	Reference
1	Identity	An identity is defined as inseparable from an individual’s sense of self and individuality. Identity can be defined by how your identity is established such as physical or biometric identifiers (e.g. photographs and fingerprints), written identifiers (e.g. drivers’ licences and passports), financial identifiers (e.g. bank account, credit card and employment information), and digital identifies (e.g. user Id and authentication used on information systems, websites, applications, and devices such as smartphones, tablets and laptops).	Modified *term* Cuganesan and Lacey (2003); MCLOC (2008)
	Identification Documentation	Identification documentation means any document or other thing that contains or incorporates identification information and that is capable of being used by a person for the purpose of pretending to be, or passing himself or herself off as, another person (whether living or dead, real or fictitious, or an individual or a body corporate).	MCLOC (2008)
	Identification Information	Identification information means information relating to a person (whether living or dead, real or fictitious, or an individual or a body corporate) that is capable of being used (whether alone or in conjunction with other information) to identify or purportedly identify the person, and includes the following: <a list of attributes>	MCLOC (2008)
2 – IC2	Identity Trading	The trading of identification documentation and/or identification information with the intention of committing, or facilitating the commission of, an indictable offence.	New
3 – IC3	Identification Equipment	The possession of equipment that is capable of being used to make or modify identification documentation with the intention of committing, or facilitating the commission of, an indictable offence.	MCLOC (2008)
4	Identity Takeover	The assumption of a pre-existing identity (or significant part thereof), with or without consent and, whether, in the case of an individual, the person is living or deceased.	Modified *term* in ACPR and AUSTRAC (2006); MCLOC (2008)

No	Identification Definition	Description	Reference
5	Identity Manipulation	The alteration of an existing identity.	ACPR and AUSTRAC (2006); MCLOC (2008)
6	Identity Fabrication	The creation a fictitious identity.	ACPR and AUSTRAC (2006); MCLOC (2008)
7	Identity Theft	The theft of a pre-existing identity (or significant part thereof) without consent and, whether, in the case of an individual, the person is living or deceased.	Modified *term* in ACPR and AUSTRAC (2006) & MCLOC (2008)
8	Identity Deception	Misrepresentation through: (i) Creation of a false identity or changes to an existing identity through alteration of existing data, or the context of the data, relating to the identification of a real individual or entity, such as via a change of name, change of initials, change of residency details, change of date of birth etc.; and/or (ii) Creation of a false identity based on fake (i.e. fictitious) identification data; and/or (iii) Creation of false identification documentation both novel and counterfeit.	Jamieson et al. (2012)
9	Identity Fraud	The gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity.	ACPR and AUSTRAC (2006); MCLOC (2008)
10	Identity Crime	A generic term to describe activities and offences linked to dealing, collecting, trading, misusing, taking over, manipulating, fabricating, or the making of an identity to facilitate the commission of crime.	Modified *term* in ACPR and AUSTRAC (2006) & MCLOC (2008)
11 – IC1	Collection of Identification Information and Documentation	The entity facilitates the methods that are used to collect identification information and identification documentations.	New
12	Identity Related Crimes	Crimes enabled by identity crime where the purpose of the perpetrator is to seek anonymity, avoid detection, or shift the blame.	Jamieson et al. (2012)

CONSTRUCTION OF TAXONOMY

We first discuss the construction of the Hierarchy of Identity Fraud and its entities shown in Figure 2. The numbers in Figure 2 are referenced to show how the terms are associated, and the entities are displayed in italics.

Identity, Identification Information and Identification Documentation

In Figure 2, *Identity*, *Identification Information* and *Identification Documentation* (No 1 (Green box) in Figure 2) are identity objects embedded inside oval of Identity Crime, and thus, they are embedded in the taxonomy. In other words, the compromise of any the identity objects is treated as identity offences.

For example - a birth certificate can be used to validate an *identity*. Information on a birth certificate includes name, date of birth, place of birth, country of birth and parents' names and is known as *identification information* (1). Registry of Birth, Death and Marriage (BD&M - a government agency) issues the birth certificate to an individual. The birth certificate issued by the BD&M is example of *identification document* (1). A copy of the birth certificate (more likely in an electronic form) is kept by BD&M and the paper copy is given to the individual's parents.

Hierarchy of Identity Fraud

Developing the Hierarchy of Identity Fraud (see Figure 3) for identity offences was initially based on two conceptual models, namely Jamieson et al. (2008, 2012), and Sproule and Archer (2007). With the exception of *identity takeover* (4), both models discussed *identity theft* (7) and *identity deception* (8), which is described as either create a fictitious identity or manipulate one's identity.

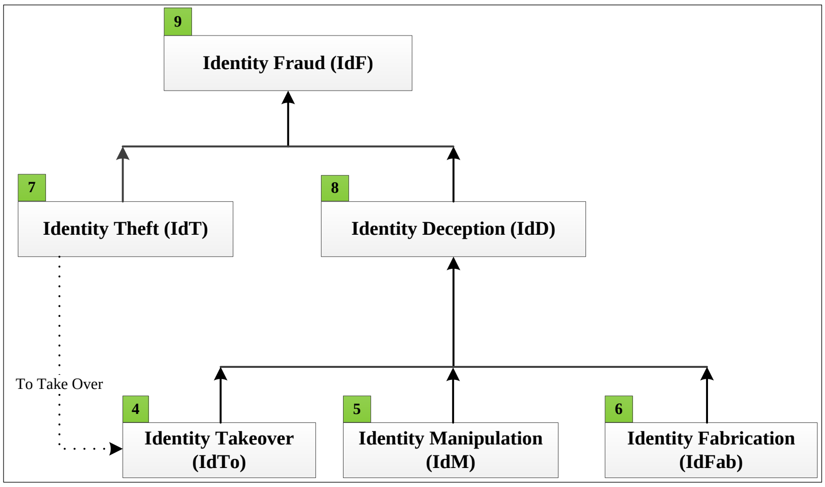

Figure 3: Hierarchy of Identity Fraud

The *Identity Theft* (7) is originally defined in ACPR and AUSTRAC (2006, p.13) as "*the theft or assumption of a pre-existing identity* (or significant part thereof)…" However, we consider "*theft of a pre-existing identity*", and "*assumption of a pre-existing identity*" as two different activities. "Pre-existing" identity assumes that no part (at least majority) of that identity has been manipulated. The conjunction 'or' links both activities together under *Identity Theft*, and it is difficult to distinguish between these criminal activities. This leads us to revise *identity theft* as pure theft of an identity (7); that is, stealing an identity usually for the purpose of committing a crime. There are conceivably criminals who steal identities for the purpose of trading them in the 'black' market. Therefore, we distinguish between stealing an identity for different immediate purposes – assume another individual's identity for an awaiting criminal activity, or for further trading of that identity.

The term *identity takeover* (4) is used to describe "*assumption of a pre-existing identity*" This refers to a perpetrator taking over a pre-existing identity through either stealing or purchasing another individual's identity. The pre-existing identity may subsequently be manipulated by modifying an attribute such as changing the individual's photograph but retaining a significant part of the pre-existing identity such as names and address. The link between (7) and (4) displays when an identity is stolen and then taken over by another person.

This taxonomy at large assumes that an identity offence is created when individuals' *Identification Information* and *Identification Documentation* are "involuntarily" exposed to some parties, which in turn, use their identity information for some gains, at the costs of the individuals. On the other hand, in the online environment, such as social media (e.g. Facebook), individuals are getting increasingly willing to "voluntarily" disclose, if not to leak, identity information (despite the expected costs and harm). Indeed, social applications (applications available on Facebook) have recently implemented some "impersonation" features, which essentially allow voluntary *identity takeover* (4). Such examples include the perpetrators have impersonated their victims in Facebook to get money from their friends (see Sutter and Carroll 2009), or a perpetrator has created an account for this victim on the Facebook to purposely defame his victim.

Identity Deception

We organise *identity takeover* (4), *identity fabrication* (5) and *identity manipulation* (6) to be subcategories of *identity deception* (8) as all these terms are related to deceiving someone with a falsified identity. *Identity Fabrication* takes place when an identity is fabricated. A fictitious identity is constructed by assembling parts from other identities or by constructing fully (partially) from scratch. However, occasionally by coincidence, a fictitious name might be similar to an existing name, especially when using a common surname such as Li and Zhang (Chinese), Kim (Korean), Nguyen (Vietnamese), and Smith and Jones (Australia/UK). When fabricating an identity, a few of the attributes used might be real such as a photograph taken from another website.

Unlike *identity fabrication* (5), *Identity manipulation* (6) starts with an existing identity but some attributes (such as name, birth place, and education qualification) are altered to create a new identity. *Identity manipulation* sometimes is also known as *identity change*. For example, a 17 year old teenage might change the date of birth on his/her driving license (can be used to prove age of the individual) so (s)he can legally consume alcohol.

Occasionally, without knowing the background and nature of an identity offence, it is sometimes difficult to know if an identity has been taken over, fabricated or manipulated. In this case, the recommendation is to classify the offence as an *identity deception*. If more information becomes available, it can be classified further.

Hierarchy of Identity Fraud and Identification Equipment Entity

Identification equipment entity (3 [IC3]) shown in Figure 4 is used to make or modify *identification documentation*. Making *identification documentation* is associated with *identity theft* (7) and *identity deception* (8) in the Hierarchy of Identity Fraud. For instance, perpetrators steal a database which contains a set of credit card numbers (7). They use a credit card making machine to produce new credit cards with stolen credit card numbers (3 [IC3]). Subsequently, they may use the credit cards to purchase goods or trade the credit cards.

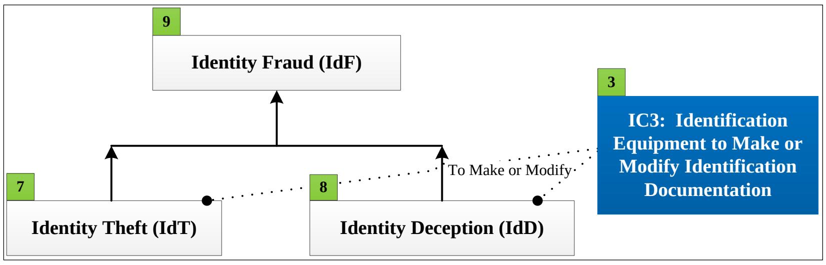

Figure 4: Hierarchy of Identity Fraud and Identification Equipment Entity

As for *identity deception* (8), an example is perpetrators using a purposely built passport equipment to make fake passports. Alternatively, the machine or equipment (3 [IC3]) can be used to modify an identity document. Other examples include making fake driving licences. A fake driving licence might have real attributes such as name and photograph but a fake date of birth (5).

Hierarchy of Identity Fraud and Collection of Identity Elements

In Figure 5, the (11 [IC1]) Collection of Identification Information and Identification Documentation provides the methods of collecting of identities, which can either be in the form of *physical*, *transaction* or *digital*. A more general term "collecting" is used instead of "stealing" because it covers a wider scope of how an identity can be obtained. For instance, if a passport is found on the floor in an airport (this is not stealing), instead of giving it to the appropriate authority, the person decides to keep the passport with the intention to sell or give it to someone else to use. To constitute an *identity theft* (7), an identity has to be collected.

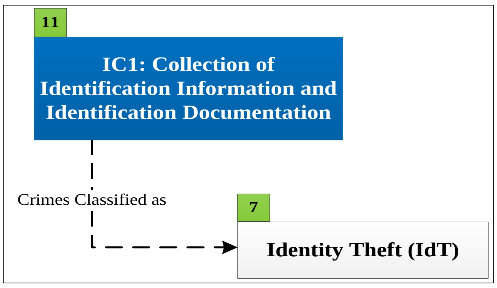
11
IC1: Collection of Identification Information and Identification Documentation
Crimes Classified as
7
Identity Theft (IdT)

Figure 5: Identity Theft and Collection of Identity Elements Entity

Hierarchy of Identity Fraud and Identity Trading

Identity trading (2 [IC2]) is essentially the exchange of identification information and identification documents for something else such as digital (e.g. BitCoins) or real currencies; or illegal items (e.g. drugs). There are a number of ways trading can take place such as via physical exchange or an online order over the Internet. Websites such as "dark web", '*an online haven for anyone looking to buy or sell drugs, weapons or other illegal goods*' (see http://www.cbc.ca/news/world/story/2013/05/02/dark-web-illegal-goods-global.html), facilitates online trading of identities.

Figure 6 shows the relationship between identity trading (2 [IC2]) and the Hierarchy of Identity Fraud. Here, we assume that the identification information and identification documents that are traded are either stolen (7) or created with fabricated identities (8).

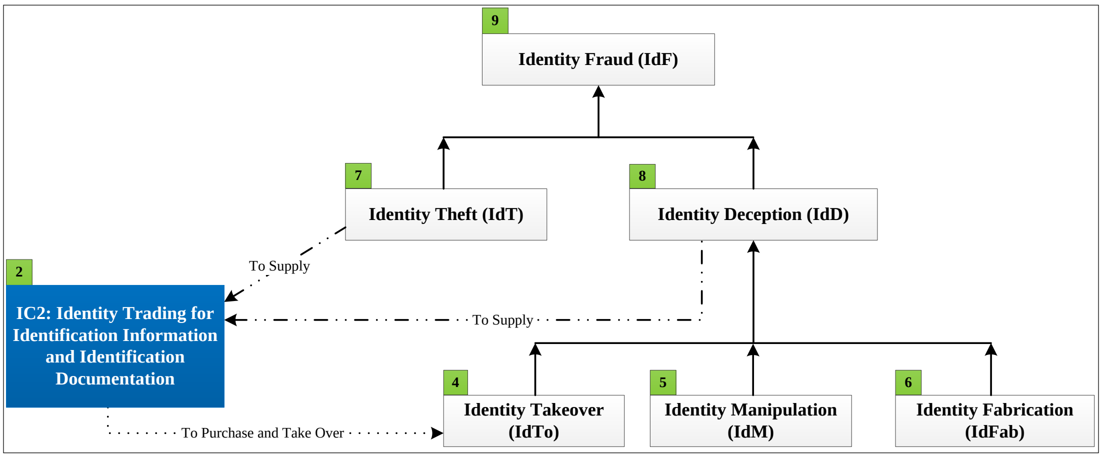
9
Identity Fraud (IdF)
7
Identity Theft (IdT)
8
Identity Deception (IdD)
To Supply
2
IC2: Identity Trading for Identification Information and Identification Documentation
To Supply
4
Identity Takeover (IdTo)
5
Identity Manipulation (IdM)
6
Identity Fabrication (IdFab)
To Purchase and Take Over

Figure 6: Hierarchy of Identity Fraud and Identity Trading

After a piece of *identification information* or an *identification document* is traded (2 [IC2]), the identity is taken over by the new owner (4). This is presented by the link between (2 [IC2]) and (4) in Figure 6.

It is sometimes difficult to distinguish if an identification document is stolen or fabricated. A person commits identity trading (2 [IC2]) if (s)he deliberately gives his/her passport to a relative to travel to Australia illegally, even though no money has been exchanged.

Identity Crime

Figure 2 summarises the coverage of *identity crime* (10) and demonstrates the complexity of identity crime - the relationships between the four key components - Hierarchy of Identity Fraud and three entities. Identity crimes can be committed in many different combinations (in terms of methods/mechanisms) and sequences (in terms of chronology).

The taxonomy shows an identification document can be stolen (11 [IC1]) and (3 [IC3]) and then traded (2 [IC2]). An identification document can be fabricated (6), and then made using equipment (3 [IC3]). All these activities are considered as *identity crime* (10). Moreover, different (identity and non-identity) crimes can further be combined and intertwined to make up a complex chain of crimes.

The complexity of these crimes can be measured in terms of the size of the crimes (e.g. financial or non-financial impact) as well as the geographical and virtual spread of these crimes. Given identity crimes can be mixed with non-identity crimes, we next describe identity related crimes.

Identity Related Crime

To complicate identity offences further, most of the offences committed are not isolated, they are linked or are under the umbrella of serious crimes such as terrorism, money laundering, and trafficking (people, drugs, weapons, illicit material) (Jamieson et al. 2008). The crimes not considered as identity crimes are outside the oval of *identity crime* (10) shown in Figure 2. Identity crime is usually the ‘enabler’ in a chain of crimes. Thus, it is sometimes difficult to separate a ‘pure’ identity crime from these serious crimes which might include identity crime as one of the offences.

An identity offence is normally not just related to the misuse of an identity but it is also associated with other types of crimes such as theft, cybercrimes, money laundering, terrorism, and trafficking of people drugs, weapons, or illicit material. Misuse of an identity might only play a small part in a chain of crimes. Therefore, an *identity related crime* (12), shown in Figure 2, is basically committing an identity offence through misusing identity details of an individual or entity obtained via theft or deception in a chain of crimes (Jamieson et al. 2008).

CONCLUSION, LIMITATIONS AND FUTURE STUDY

This study has developed a taxonomy for classifying Identity Offences. It is embedded within an Identity Offences Taxonomy and serves as a valuable tool in creating a common reference point for identifying identity (related) crimes. A key of this taxonomy is its interoperability with other states and territories across Australia and indeed there is a significant correlation with international governments. This research study is only the beginning for developing a holistic vision and strategies for managing identity crimes in Australia. Within the field of Information Systems, the use of Information Systems to manage identity offences has a particular significance. Just as the ubiquity of computers and the Internet with over two billion users makes Information Systems critically susceptible to the abuse of false personal and organizational identities, Information Systems also (potentially) holds promises for managing, controlling and preventing identity crimes. There is emerging evidence of this through both government practices within Australia and abroad, as well as in private institutions. For example, increasingly, secure online identity verification systems are deemed a necessity before consumers/citizens will willingly participate in online transactions. There is a move towards online identity checking as part of the identity ecosystem.

Online government or e-government services (e.g. online medical records, healthcare Medicare claims, and online immigration records) are increasingly provided by the Australian government (see MyGov 2014). Emerging technologies such as Forensics Live Acquisition systems also promise to gather live data without shutting systems down, while illegal activities such as identity crimes are taking place; these data serve as evidence in court and this innovation is crucial as a deterrent for these crimes. However, due to confidentiality and privacy laws, and the complexity of such systems, the adoption and implementation of such systems are not straightforward.

The taxonomy presented is a result of an analysis of definitions used within Australia (although we also saw many similarities with those used in many countries such as US and Canada). Further research is required to see if the taxonomy can be applied to other countries.

Given the extent and cost of identity offences, a comprehensive approach is required to understand the ongoing status of different types of identity offences committed. In Australia, this has not been possible until we understand and agree upon a common frame of reference across all the different states and government agencies. A clarity in the structure of identity offences help governments and businesses measure and track identity (related) crimes in a consistent way. This makes possible more accurate and realistic planning and implementation of identity crime management. However, given the nature of the rapid changes in technologies, we can only make true progress when current law continue to be reinforced, laws be amended, and new identity crimes laws be constructed (Jamieson et al. 2012). Furthermore, the mechanisms used by perpetrators are often multifaceted – technical, psychological, physical – thereby necessitating a multidisciplinary approach to identity crime management.

The literature also informs us that amongst other purposes (see Land et al. 2013), the taxonomy will assist in theory building (Bapna et al. 2004; Nickerson et al. 2013). This article presents a first effort in exploring and creating that taxonomy. In its current state, this taxonomy serves to map out different research agendas to study different classes of identity offences. It is still too premature to claim theory building at this point. Further drilling down of the taxonomy is needed to create different research programs which can inform different theories to understand different types of identity offences. For example, romance crimes can be studied from the perspectives of victims, perpetrators, and service providers of online dating organisations to understand the behaviours/reactions of different stakeholders (Pan et al. 2010).

We encourage Information Systems researchers stand in good stead to drive this research agenda, since the technological component plays a huge role in combat and the facilitation and combat of such crimes. Future research should naturally involve researchers from multiple disciplines such as Law, Psychology, Computer Science and Information Systems. Researchers from multidiscipline can advance the field through collaborations.

REFERENCES

ACPR (The Australasian Centre for Policing Research) and AUSTRAC (The Australian Transaction Reports and Analysis Centre) 2006. “Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency.” Retrieved 5 November, 2012, from http://www.acpr.gov.au.

Australian Bureau of Statistics, 2012. “Personal Fraud Costs Australians $1.4 billion.” Retrieved 24 September, 2014, from http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/4528.0Media%20Release12010-2011?opendocument&tabname=Summary&prodno=4528.0&issue=2010-2011&num=&view=.

Bapna, R., Goes, P., Gupta, A., and Jin, Y. 2004. “User heterogeneity and its impact on electronic auction market design: An empirical exploration”, *MIS Quarterly*, (28:1), pp. 21-43.

Cuganesan, S., and Lacey, D. 2003. *Identity Fraud in Australia: An evaluation of its Nature, Cost and Extent*. SIRCA, (Securities Industry Research Centre of Asia-Pacific), Sydney.

Finklea, K., 2014. “Identity Theft: Trends and Issues.” Retrieved 31 July, 2014, from http://fas.org/sgp/crs/misc/R40599.pdf.

Jamieson, R J., Stephens, G., Winchester, D. W. 2007. "An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts," *Proceedings of the 11th Pacific Asia Conference on Information Systems (PACIS)*, 3 – 6 July, 2007, Auckland, New Zealand.

Jamieson, R., Land, L., Sarre, R., Steel, A., Stephens, G., and Winchester, D. W. 2008. "Defining Identity Crimes," *19th Australasian Conference on Information Systems*, Christchurch.

Jamieson, R., Land, L.P.W., Winchester, D., Stephens, G., Steel, A., Mauruchat, A., Sarre, R. 2012. "Addressing Identity Crime in Crime Management Information Systems: Definitions, Classification, and Empirics," *Computer Law & Security Review*, (28:4), pp 381-395.

Johns, R. 2012. *Sentencing in Fraud Cases, Monograph 37 - September, 2012*. Judicial Commission of NSW.

Land, L., Smith, S., and Pang, V. 2013. "Building a Taxonomy for Cybercrimes," *Proceedings of the 17th Pacific Asia Conference on Information Systems (PACIS)*, 18-22 June, 2013, Jeju Island, Korea.

Le Lievre, E., and Jamieson, R. 2005. "An Investigation of Identity Fraud in Australian Organizations," *CollECTeR LatAm 2005 Conference*, Chile, pp 1-10.

Mitchell, P., Hays, T., and Satter, R. 2013. "Westpac Caught up in World's Biggest Money Laundering Sting." Retrieved 29 May, 2013, from The Sydney Morning Herald.

Model Criminal Law Officers' Committee (MCLOC) of the Standing Committee of Attorneys-General (2008) "Final Report 2008 - Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General." Retrieved 25 November, 2012, from http://www.sclj.gov.au/agdbasev7wr/sclj/documents/pdf/identity_crime_final_report_march_2008.pdf.

MyGov, 2014. "About (Australian Government) MyGov." Retrieved 31 July, 2014, from https://my.gov.au/mygov/content/html/about.html.

N. A., 2014. "What is the Law on Impersonating Another Person on Facebook?" Retrieved 26 September, 2014, from http://www.inbrief.co.uk/human-rights/impersonating-someone-on-facebook.htm.

Newman, G.R., and McNally, M. M. 2005. "Identity Theft Literature Review". U.S. Department of Justice.

Nickerson, R.C., Varshney, U., and Muntermann, J. 2013. "A Method for Taxonomy Development and its Application in Information Systems," *European Journal of Information Systems* (22:3), pp 336-359.

Pan, J.A., Winchester, D., Land, L., and Watters, P. 2010. "Descriptive data mining on fraudulent online dating profiles," *18th European Conference on Information Systems (ECIS)*, Pretoria, South Africa, 7-9 June, 2010.

Sproule, S., and Archer, N. 2007. "Defining Identity Theft," in: *Eighth World Congress on the Management of eBusiness (WCMeB 2007)*, Toronto, Ontario, Canada, 2007, pp 1-11.

Straub, D. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp 255-276.

Sutter, J., and Carroll, J. 2009. "Fears of Impostors Increase on Facebook", Retrieved 6 February, 2009, from http://edition.cnn.com/2009/TECH/02/05/facebook.impostors/index.html.

Wang, G., Chen, H., and Atabakhsh, H. 2004. "Automatically Detecting Deceptive Criminal Identities," *Communications of the ACM*, (47:3), pp 71-76.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the assistance and cooperation of participants from the organisations sponsoring this Identity Fraud Linkage Research Project and to Attorney-General's Department and the Australian Research Council for their research grant.

COPYRIGHT