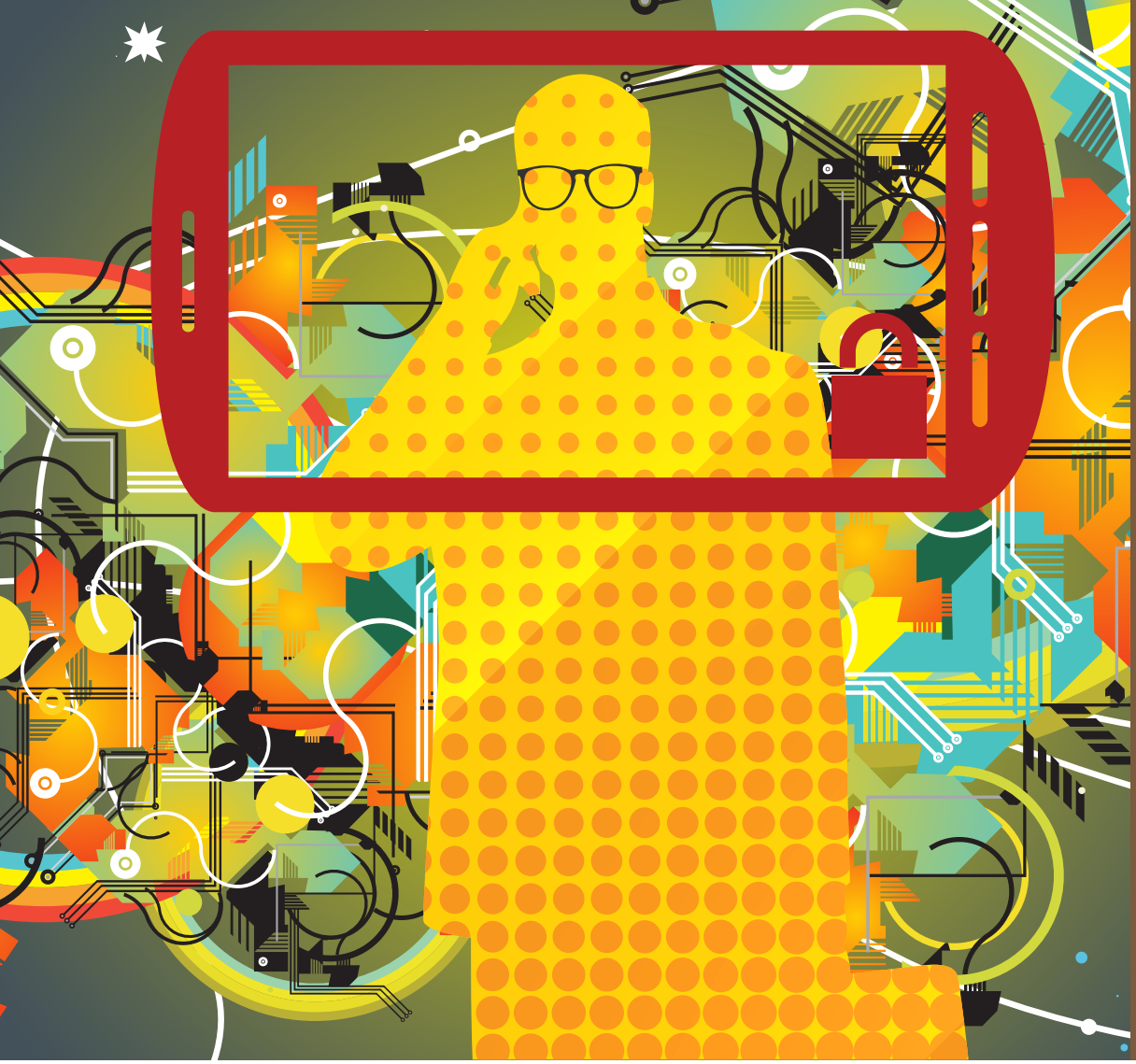


Identity theft and Australian telecommunications:

A structured literature review

Australian National University

IDCARE

ACCAN

Identity theft and Australian telecommunications:

A structured literature review

Principal concepts and a conceptual framework

Sigi Goode

May 2017

Identity theft and Australian telecommunications: A structured literature review

Authored by **Sigi Goode**

Published in **2017**

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

Australian National University
Website: http://www.anu.edu.au
Email: sigi.goode@anu.edu.au
Telephone: +61 2 6125 5048

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: +61 2 9288 4000
If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: www.relayservice.gov.au

ISBN: 978-1-921974-50-2
Cover image: Design by Richard Van Der Male with image from Shutterstock

This work can be cited as: Goode, Sigi (2017) "Identity theft and Australian telecommunications: A structured literature review", Australian Communications Consumer Action Network, Sydney.

Table of Contents

Introduction

Identity theft affects thousands of Australians every year. Recent estimates have put the number of affected Australian citizens at 770,000 in 2015, with almost one in five Australians having their personal information stolen or compromised at some point in their life (Veda Group 2015). A number of identity theft threats exist, generally revolving around the illegal access to personal and financial information: while such identity theft has traditionally involved the physical theft of identity documents and personal mail, newer attacks are moving to electronic means, such as online social media and other information communications tools and services (e.g. smartphones) to collect identity information. Perpetrators then use this information to drain their victims' bank accounts, impersonate them online, secure loans, or commit other frauds such as blackmail and extortion. Countries around the world, such as the United States and United Kingdom, are also working to understand and overcome this international threat.

In August 2016, researchers at the Australian National University partnered with IDCare, Australia's identity support service, to undertake a research project for the Australian Communications Consumer Action Network (ACCAN). This research project aims to better understand identity theft victim reporting in Australia, and especially the role played by information and communications technology in identity theft attacks.

This report, the first to be produced in the project, represents the foundational theoretical framework for the project. This document provides a review of prior research knowledge regarding identity theft, based on completed research studies published in international research journals. The report synthesizes approximately 200 research articles across a range of disciplinary areas. The report identifies conceptual themes in prior literature and also identifies gaps in understanding and knowledge. The document then develops a conceptual framework to organise this prior literature, and a nomological network to identify the paths of enquiry that will form the basis of the next stage of the research project. The document hence represents the first step of the subsequent study into identity theft commission and detection in Australia.

Sigi Goode (Research School of Management, ANU, 2017)

Methodology

We first conducted a structured literature review of prior research into identity theft. Our philosophical goals in conducting this literature review were threefold. First, we sought to holistically understand current conceptual knowledge regarding identity theft. Because different disciplines might evidence different perspectives and types of knowledge regarding identity theft, a multidisciplinary search across literature bases was needed. Second, we wanted to identify and better understand the gaps in present knowledge. Third, we sought to develop a conceptual and methodological framework that could be used to inform our subsequent data analysis approaches in later stages of the project.

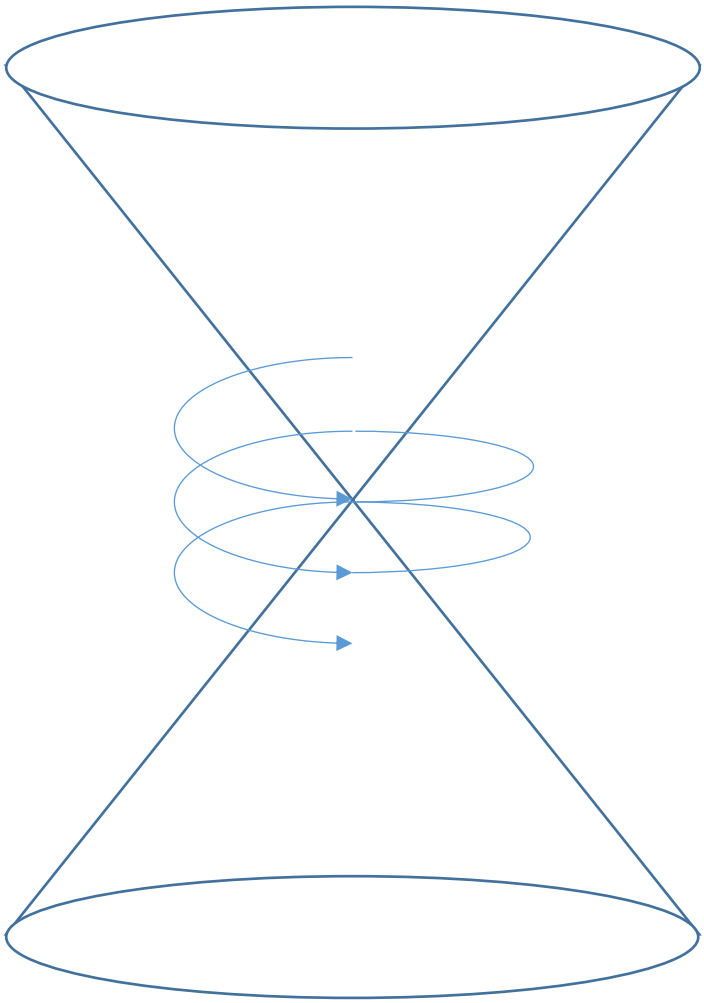
We used a multi-stage approach to finding articles in the literature review. We took a multidisciplinary view of the nature of identity theft, as recommended by Halperin and Backhouse (2008). Following further recommendations from Smith et al. (1996) and Smith et al. (2011), we aimed to be as inclusive as possible in our literature search and so took a broad approach to finding literature sources: accordingly, we did not restrict our search to any particular disciplinary area. We sought a well-founded basis on which to categorise and synthesize prior work and hence we sought only completed studies in published journal articles.

The first step was to collect and collate an initial corpus of research literature. To do this, we used a set of conceptual 'seeds' from which to grow a larger literature corpus. To begin, we used a keyword search to identify an initial group of relevant papers in prior identity theft literature. We used search terms to describe identity theft based on the labels discussed by Jamieson et al. (2012), including "identity theft", "identity crime", "identity takeover", "false identification", "passport fraud" and others. We accepted all papers published up to and including 2016. This process provided an initial group of key research papers; we reviewed these papers in order to identify additional relevant identity theft terms, and then used these terms in a large scale literature search across major literature search engines including Google Scholar, Scopus and EBSCO. This initial search yielded a group of 2482 papers.

The second step involved refining the literature corpus. From this initial group of papers, we eliminated duplicate papers, and articles that did not focus substantially on identity theft as a criminal activity. For example, many papers used identity theft to justify other work (such as research into encryption, botnets and botnet detection). Some papers used the term "identity theft" when discussing the appropriation of a historical, national or antique culture (e.g. Gleason 2011; Mazzarella 2004; Noy 2009). Third, a number of papers cited identity theft as a potential weakness when developing identity-based and identity-dependent systems, such as large-scale databases or smart card implementations. We excluded these types of papers from the literature corpus on the basis that they did not substantially address the concept of identity theft itself. This step left us with 216 core papers that formed the basis of our literature corpus.

We obtained, read and summarised each paper in the corpus. We identified concepts using an iterative process to switch to and from our library of concepts and the literature articles, following advice from Webster and Watson (2002) regarding processes for conceptual identification. As we read each paper, we searched our concept library in order to identify relevant concepts. Then, we amended the concept bank in turn to include the new concepts arising from each paper. This iterative approach allowed us to grow the concept library while remaining faithful to the literature at hand.

The third step was a process of conceptual application. From our structured literature corpus, we returned to the wider literature base in order to observe how these concepts were being applied and discussed in the wider literature. This stage was useful for three reasons. First, it yielded a richer basis of conceptual understanding. Second, it allowed us to understand how these concepts were being applied practically. Third, it allowed us to identify studies that spanned multiple conceptual categories. The rest of this report describes this conceptual application in the wider literature.



Literature Collation

Purpose: identify a wide area of published research

Method: keyword searching to drive an initial collection, followed by sub-searching and citation tracking

Literature Refinement

Purpose: identify conceptual themes in published research

Method: read through core identity theft papers to identify core concepts, iterating between papers and conceptual library

Conceptual Application

Purpose: identify conceptual application and use in wider research literature

Method: read through articles in wider literature to understand how concepts are applied.

Figure 1 Literature search approach

A Structural Analysis of Prior Literature

We first present a structural analysis of the more than 200 research articles that comprised our literature corpus. These research articles were published in journals across a range of disciplinary areas. Table 1 shows the breakdown of the top 15 discipline areas. Computer Science was the most popular field, followed closely by Criminology. Interestingly, despite mention of medical identity theft in the popular literature, only five journals in the Health and Medicine category published articles that focused on identity theft.

Table 1 Disciplinary areas of journals publishing identity theft studies

Discipline	n	Discipline	n
Computer Science	32	Health and Medicine	5
Criminology	27	Psychology	5
Information Systems	21	Sociology	5
Law	20	Applied Economics	4
Library and Information Studies	8	Communications Technologies	3
Marketing	7	Engineering	3
Policy and Administration	7	Anthropology	2
Business and Management	6		

The literature corpus spanned the period 1999 to 2016. Figure 2 shows that the number of published identity theft studies has been growing. Only one paper in our literature corpus was published in 1998, but this number had grown to 18 papers by 2010. Early papers tended to be from the telecommunications field. By 2004, the number of fields publishing research into identity theft had grown to six in our corpus.

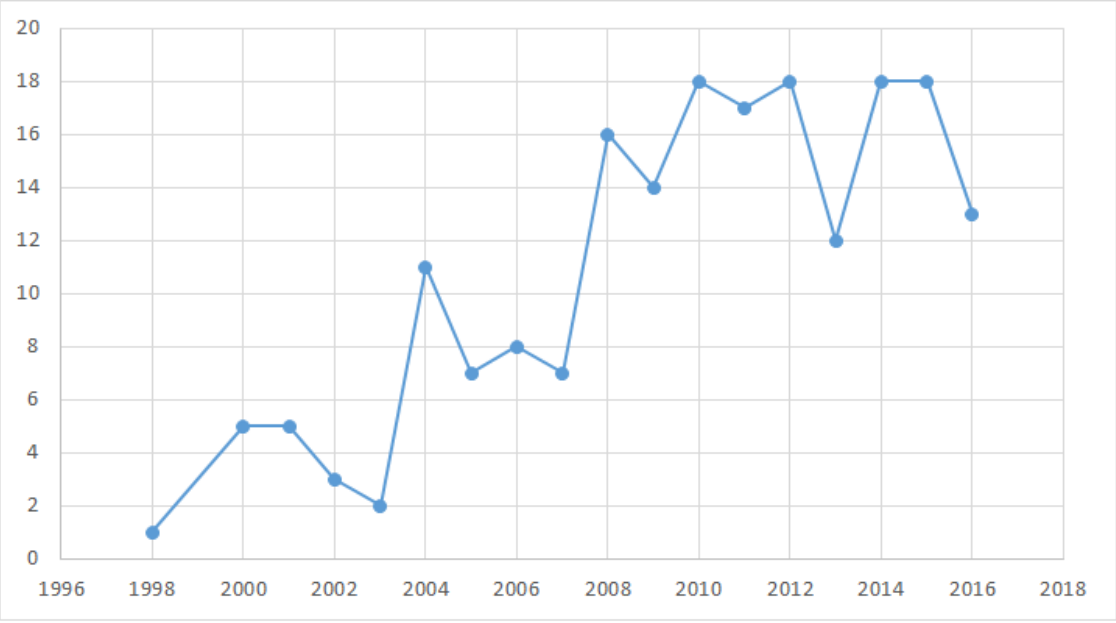


Figure 2 Frequency of publication of identity theft research articles, by year

Major Concepts in Prior Literature

As discussed above, we reviewed each paper in order to determine salient concepts. We iterated between papers and the library of concepts in order to make sure that the library accurately reflected their development in prior literature. Fundamentally, prior literature on identity theft is disaggregated and still largely immature (Eisenstein 2008; Anderson 2006; H. Copes et al. 2010). While the number of published research works into identity theft is increasing, theory and concepts are still developing and it remains difficult to identify clear lines of argument development through prior literature. In total, we found a number of concepts which we grouped into 14 main clusters. These conceptual clusters are discussed below.

Conceptualising the victim

Accessing identity theft victims in order to understand their behavioural makeup is a challenge for identity theft research, echoing difficulties in information security research more broadly. We could find only a small number of papers in the corpus that focused on this aspect of identity theft. Clearly, there is also an inherent bias in identifying identity theft victims, as with all security research, in that only identified victims can be studied: further, guilt, shame, and embarrassment may prevent many of these individuals from participating in such studies (von Lampe 2008; Heith Copes, Vieraitis, and Jochum 2007; Deem 2000; Van der Meulen and Koops 2011). Typically, most research into identity theft victims takes place long after the identity theft incident itself, which may also affect respondents' ability to recall events and behaviours. Understanding victim behaviours, activities, and pathologies yet requires more work.

Prior research conceptualises the identity theft victim in several different ways. Most prior research into identity theft adopts an implicit conceptualisation of the victim of an identity theft attack. Consumers, generally, are seen as especially attractive targets for identity theft, first because they are likely to have access to identity credentials, identity verification knowledge, and financial resources (Marron 2008; Lacey and Cuganesan 2004), and second because they may be untrained and uninformed about procedures and risks (Butler 2007; Gilbert and Archer 2011; Seda 2014; Albrecht, Albrecht, and Tzafrir 2011). The victim is sometimes portrayed as unlucky or careless with their identity credentials (Hoar 2001; Hinde 2003; Whitson and Haggerty 2008; Siegel 2006; Whitson and Haggerty 2007; Kirk 2014). In some cases, the victim is also careless with identity tokens, with the information systems that hold this identity information, and through poor device use or poor password selection (Hinde 2003; Hinde 2005; Furnell 2010). Importantly, much of this work emphasizes the point that while it would be easy to blame such victims for being at least partly complicit in the identity theft attack, through inattention, ignorance, misunderstanding or sometimes direct misuse (Furnell 2010) this blame is not always appropriate (H. Copes et al. 2013). Victims are, in the main, seen as rational, informed actors (Turner, van Zoonen, and Harvey 2014), but a set of core factors likely exacerbates the risk of becoming a victim of identity theft, including certain demographic characteristics (Anderson 2006), risky activities, insufficient precautions (Anderson 2006) and reluctance to report suspicious activity (H. Copes et al. 2010; K. Holtfreter et al. 2015). Also, there is evidence that online users, at least initially, are often unaware of the risk of identity theft (Tow, Dell, and Venable 2010; K. Holtfreter et al. 2015; Furnell 2010): in contrast, some of these online users actually proactively advertise their most important attributes, activities and features to strangers in order to acquire social popularity (Furnell and Botha 2011), regardless of the perceived risk to their personal information and privacy (J. Chen

et al. 2014; Venkatanathan et al. 2014). Experimental work has shown that online users may become even more risk-seeking if they are aware that identity protection measures are in place (Poindexter, Earp, and Baumer 2006), possibly because they overestimate the effectiveness of electronic identity theft countermeasures (Dilla et al. 2013).

In other cases, the victim is conceptualised as unaware and remote from the attack. In this stream of research, the victim does not play a significant active role in the identity theft incident: instead, their identity details are obtained through a third party such as a service provider or social network (Patsakis et al. 2015; Patsakis et al. 2014; Fire, Goldschmidt, and Elovici 2014; Norouzizadeh Dezfouli et al. 2016), are stolen before the victim receives them (Mercuri 2006), or are fabricated without the victim's involvement (Marron 2008; Jamieson et al. 2012; Seda 2014). In some cases, the identity thief may create a viable composite identity using identity credentials and documentation from a variety of victims (Phua et al. 2012). In this vein, some early work argued that customers ought to bear the principal burden of combating identity theft (A. D. Smith 2005): this may be because early incidents of identity theft were overwhelmingly undertaken with paper-based documentation rather than via computer technology (Mercuri 2006; Halperin and Backhouse 2008), and customers were better able to protect these paper-based documents.

In comparison, a very small amount of research explicitly conceptualises the identity theft victim. These studies typologise the victim by explaining their identity characteristics, usually in order to explain in general terms how they were involved in the identity theft and their role in recovering from the attack (Whitson and Haggerty 2008). The majority of such research is based on North American data and case files. Demographically, profiles of victims in prior work seem mixed:

- Those who are female, black, young, and low income are disproportionately victimised by existing bank account fraud (H. Copes et al. 2010)
- Males, older individuals, and higher income earners were more likely to be identity theft victims (B. W. Reyns 2013)
- Victims tended to be white and male (Allison, Schuck, and Lersch 2005)
- The risk of identity theft appears to be higher for people with higher incomes, younger consumers, and females (Anderson 2006)

Behaviourally, profiles of victims seem more consistent:

- Individuals who use the internet for banking, emailing and instant messaging are 50% more likely to become identity theft victims (B. W. Reyns 2013)
- Users with lower self-efficacy are less able to avoid phishing attempts (Arachchilage and Love 2014)
- Females were less concerned about identity theft risks when purchasing online (Predmore et al. 2007)

Broadly, there is evidence that socio-demographic factors can explain at least some identity theft victimhood. For instance, race and ethnic background appears to affect victim propensity (Lane and Sui 2010) – accordingly, geographical location of the victim also has a bearing on how the victim is initially attacked, possibly because this factor affects where they conduct their business (Anderson 2006). Cultural background also appears to have an effect on awareness of and predisposition towards identity theft (Al-

Hamar, Dawson, and Al-Hamar 2011; Keaney 2009), possibly due to varying norms of trust in these cultures (Crompton 2010).

Identity credentials and documentation

Comparatively few papers focused exclusively on identity credentials alone – most research work discussed identity documentation within the context of a particular crime or industry. Research papers that did focus on the theme of identity credentials could be divided into four subgroups. First, numerous papers discussed the role of identity credentials in an identity theft attack (often without specifying or analysing the nature of those credentials). A prominent theme in this stream of research is that the success of the identity theft attack is heavily influenced by the type of identity credential available to the attacker (LoPucki 2001; Marshall and Tompsett 2005; Sovern 2002; Lai, Li, and Hsieh 2012). More extensive and personally intimate identity details afforded the attacker a wider array of abilities and opportunities in committing fraud (H. Copes and Vieraitis 2009). Accordingly, research in this stream sometimes highlights the importance of certain types of identity documents in identity theft, such as social security numbers (Berghel 2000; Acquisti and Gross 2009; Neumann 1997; Puckett 2009), but further work is needed to understand how such documentation is actually used in subsequent frauds.

A second stream of research focused on which identity credentials have been popular in identity theft attacks. Government-issued photographic identity documents, such as passports and driver licences, appeared to be the most popular identity credentials sought by identity thieves (Rudner 2008; Grijpink 2005) possibly because these credentials afforded the attacker the easiest and fastest method for exacting a financial benefit (Lynch 2005; Marshall and Tompsett 2005; Angell 2008; R. G. Smith and Budd 2009; Barraclough et al. 2013), because these documents allow the identity thief to conceal their own identity (Allison, Schuck, and Lersch 2005), and because government-issued identity documentation is deemed highly trustworthy. Banking and payment details, especially credit card and bank account numbers (Kahn and Roberds 2008), are also commonly targeted.

A third stream of research tended to focus on developing more robust identity documents, particularly for use in online transaction environments (Marshall and Tompsett 2005; Berghel 2000; A. D. Smith 2005). The development of more secure computer login methods, particularly stronger passwords, has been a prominent theme in this work (Bang et al. 2012; L. Zhang and McDowell 2009). Other studies of this type have examined the use of biometric identity management systems, in which either a user's particular bodily features (e.g. facial features, fingerprints) or behavioural idiosyncrasies (e.g. typing speed or keystroke frequency) are used to verify or identify individuals (Ngugi, Kahn, and Tremaine 2011; Grijpink 2005). A number of studies have since questioned the privacy implications and identity theft prevention benefits of such initiatives (Grijpink 2006; E. A. Whitley and Hosein 2008; Chollet et al. 2012; M. L. Johnson 2004).

As a reaction to the multitude of identity documents needed by a citizen in their daily life, another stream of research has focused on the development of national identity cards. Such cards are designed to securely store a selection of identity tokens that can be used to access government and some private services (E. A. Whitley et al. 2007; M. Jackson and Ligertwood 2006). Examples of such cards include the Australia Card (Cradduck and McCullagh 2008), the Malaysian MyKad card (W. H. Loo, Yeow, and Chong 2011) and the UK Identity Card (C. Sullivan 2008). Ethical and privacy concerns regarding these implementations persist (Joinson et al. 2006; Neumann and Weinstein 2001), despite not all of these examples still being in use.

A fifth stream of research focuses on the use of third-party provided documentation to verify identity claims. Typically, this approach involves the use of authorised third party identity documentation such as a driver's licence, passport or biometric passport upon account creation and again at the point of customer contact (Judson, Haas, and Lagu 2014; Grijpink 2005; He et al. 2014; Modi et al. 2013) where these identity tokens are furnished by a first party, presented by a second party, and validated by a third party (W. Wang, Yuan, and Archer 2006). Despite concerns regarding privacy threats and technical weaknesses in federated identity management systems (Hansen et al. 2004; Madsen and Itoh 2009), particularly among third party providers, there remains a strong voice in the literature regarding the benefits of such systems, including more economical security arrangements, more consistent developer tools and procedures, and easier deployment in new environments (Cavoukian 2008; Torres, Nogueira, and Pujolle 2013). The cloud computing industry, in particular, has been a theatre for this type of research (Bhargav-Spantzel, Squicciarini, and Bertino 2006; Ghazizadeh et al. 2012; Sengupta, Kaulgud, and Sharma 2011). Identity federation, whereby an individual can access multiple protected systems using a single set of identity credentials, has also been identified as a practical solution to the problem of users holding multiple identities in the online space (Damiani, di Vimercati, and Samarati 2003) given that such behaviour makes it difficult to keep all such identifies secure. Holding multiple identifies can compromise trust between transaction partners, especially if third parties are involved (Satchell et al. 2011; Smedinghoff 2012): other research along these lines examines the role of third party trust seals in improving perceptions of and ameliorating the risk of identity theft in online transactions (Jiang, Jones, and Javie 2008).

Conceptualising the attacker

The identity thief is at the heart of an identity theft attack, however very little research has focused on understanding and conceptualising the nature of the identity theft instigator (Allison, Schuck, and Lersch 2005; Sharp et al. 2004). Most research into identity theft yielded very general descriptions of identity thieves, if they described the attacker at all (H. Copes and Vieraitis 2009). This was a surprising observation, given the extent of prior work and the importance of understanding this malicious actor in the identity theft process. However, this gap underlines a critical issue in identity theft that an attacker aims to adopt another person's identity while simultaneously concealing their own. This problem may mean that a thief's identity is only known following successful apprehension and prosecution: however, in most identity theft cases, this does not occur and the culprit is never apprehended (Matejkovic and Lahey 2001; Dowe 2005; H. Copes and Vieraitis 2009). Identity theft attackers also differ from other types of perpetrators in that they cannot easily choose targets based on the amount of money they are likely to be able to obtain (Anderson 2006)

Accordingly, gaining access to real identity thieves is difficult. There is little research specifically examining the identity of identity thieves, and as with the study of identity theft victims (see above), most such research is based on North American identity theft cases. Two principal approaches exist in prior literature. The first approach relies on archival data from law enforcement. For example, Gordon et al. (2007) used selected US Secret Service cases from the period 2000 to 2006. Allison et al. (2005) used archival data from a large Florida police department. Wang et al. (2004) used criminal record data from a Tucson, Arizona police department. A number of studies use archival data from the Federal Trade Commission's (FTC) Identity Theft Clearinghouse (Romanosky, Telang, and Acquisti 2011; Higgins et al. 2008; Anderson 2006; Sylvester 2004).

The second approach requires conventional study participants to think and respond like an identity thief. For instance, a study of college students found that self-disclosed identity thieves scored higher on the Autism spectrum than other students (Seigfried-Spellar, O'Quinn, and Treadway 2015), also exhibiting poorer communication and social skills. A study of high school students found that low self-control and deviant peer association were also positively associated with expressions of identity theft behaviours (Marcum et al. 2015). However, evidence from Milne (2003) suggests that students possess lower awareness of identity theft, but overestimate its incidence. However, the degree to which such participants actually approximate real identity theft perpetrators remains unknown.

Most prior research into real identity theft investigations does not or cannot explore the identity of the perpetrator. Prior work that does mention the attacker appears to conceptualise identity theft attackers in two ways, largely on the basis of their proximity to the identity theft incident.

In the first conceptualisation, the identity thief is very close to the attack. The attacker may identify and collect the victim's credentials by hand (for example, taking a driver licence from a victim's purse, stealing credentials from a mailbox, or service staff making additional copies of a victim's credentials for later use) (Downing et al. 2016). Prior work seems to suggest that attackers of this type are easier to apprehend, partly because of their physical presence and proximity to the victim or the attack (Sovern 2002; Albrecht, Albrecht, and Tzafrir 2011). In prior work, attackers that fall into this category are typically known to the victim in some way, and typically have more ready access to their identity documentation (as discussed earlier). In some cases, the attacker either acts as or is an agent of an organisation and uses de facto authority to gain access to a victim's identity documentation. For example, the medical literature describes cases of "nurse imposters", who supply forged documentation in order to gain access to patients, and then steal patient documentation in order to commit other frauds (Murray et al. 2011).

In the second conceptualisation, the identity thief is distant from the attack, and the attacker and victim never come into physical proximity (B. W. Reyns 2013). Here, the attacker gains access to a victim's credentials perhaps by purchasing them from a third party, by exploiting a weak password or other system weakness, or even by guessing or fabricating parts of a victim's identity credentials. Prior work suggests that perpetrators of this type are harder to apprehend because of their separation from the attack. Attackers that fall into this category are not initially known to the victim, however they may become known to the victim through a variety of means including phishing and spear-phishing, cold calling, infecting the user's computer with malware, or outright demands for money or other benefits.

Among studies that use their own (usually North American) proprietary data, descriptions of actual offenders vary:

- The typical apprehended offender is African American, female, unemployed, working alone, and are unknown to victims (Allison, Schuck, and Lersch 2005)
- Offenders are mainly male, typically students, working alone, usually aged between 15 and 20 years old, and most do not have criminal records (Y. Chen et al. 2005)
- Most offenders are African American, male and aged between 25 and 34 years (Gordon et al. 2007)
- Most offenders are white, aged between 25 and 44 years of age, and were college educated (H. Copes and Vieraitis 2009)

Identity theft motives

The vast majority of prior research does not conceptualise or detail the motivations behind identity theft attacks (H. Copes et al. 2013). The primary motivation assumed in much prior literature is the desire to acquire a financial benefit (Allison, Schuck, and Lersch 2005), however there is argument that this is not always the case (Perl 2003).

Motivations other than the desire to acquire a financial benefit are also discussed, to a lesser extent. These motivations include a desire for revenge against the victim, possibly for a bad inter-personal or romantic relationship (Spitzberg and Hoobler 2002) or a bad business transaction or employment relationship (W. Wang, Yuan, and Archer 2006); the simple challenge of stealing a person's identity (Grabosky 2007); the need for a 'clean' identity through which to acquire travel documents (La Fors-Owczynik 2016; Rudner 2008); the psychological satisfaction of controlling another person (S. L. Jackson 2015); the desire to either build a reputation in criminal circles or to destroy the reputation of a victim (Hoar 2001; Romanosky, Telang, and Acquisti 2011; Lynch 2005; Solove 2003); the desire to evade police detection for an unrelated crime (G. Wang, Chen, and Atabakhsh 2004); and the simple desire to cause disruption and upheaval (Z. Zhang and Gupta 2016). Underlying some of this research is the charge that identity-dependent systems are so complex that they cannot be effectively managed, or that their weaknesses are difficult to identify (Amori 2008).

There is evidence that perpetrators go through stages of experimentation and confidence-building when attempting to acquire an identity (Albrecht, Albrecht, and Tzafrir 2011). This finding suggests that their motives may change over the course of an identity theft attack. However, the nature of these changes, if they exist, is not well understood. In the wider criminological literature, there is a stronger understanding of the relation between motives and criminal outcomes; however, the relation between motives and identity theft outcomes requires further research.

Identity theft commission

The commission of identity theft has been conceptualised in a variety of ways in prior literature. The majority of prior work in this cluster provides general descriptions of how identity theft is committed. The overall picture portrayed by these studies is that a number of participating factors affect identity theft commission; however, papers typically only examine a subset of these factors in any one study. Having reviewed the literature in this area, we have grouped these factors, broadly, into three main conceptual subgroups.

The first subgroup of studies relates to the technical means of identity theft commission. Within these descriptions, the primary mechanisms for identity theft are credit card skimming, either automatically (Sproule and Archer 2010), remotely (McPhail et al. 2009) or with the face to face involvement of a checkout clerk or other credit card handler (Downing and Geller 2012; Downing et al. 2016; Mik 2012), either using automatic electronic devices (in newer literature) or by collecting credit card receipt slips (typically in older literature) (Towle 2004); dishonest or complicit retail or call centre staff (Moir and Weir 2009); inadvertent disclosure of customer information in corporate, legal or court filing documents (Caughey 2004; LoPucki 2009; M. E. Johnson 2008) or in publicly available databases such as an electoral roll or registers of company ownership (Gordon-Till 2005); inadvertent leaking of personal data through incorrectly configured or malicious system and device features (A. Loo 2009; Ahmadinejad and Fong 2014; Madhusudhan and Mittal 2012); inadvertent leaking of personal information through incorrect disposal of

data storage devices (Jones et al. 2009; Bennison and Lasher 2005); among users of online systems such as online dating tools (Rege 2009), job and employment boards (Sweeney 2006), multiplayer network games (Y. Chen et al. 2005), and virtual worlds (Dilla et al. 2013), especially when virtual game items can be bought and sold (Woo, Choi, and Kim 2012); phishing and spear-phishing, involving collecting a person's details electronically using a phony email message or letter (Bose and Leung 2014; Ramanathan and Wechsler 2013); and keystroke snooping, typically by way of malicious software, Trojan horses, viruses and other malware installed on the victim's computer (Mercuri 2006; Eisenstein 2008).

The second subgroup of commission-related studies relates to human level factors. These factors describe human relationship concepts that contribute to the commission of identity theft. Prior work argues that identity theft perpetrators are often known to the victims (Finn and Banach 2000; Perl 2003; Philpott 2006; Van der Meulen and Koops 2011; Southworth et al. 2007) as room-mates, friends, ex-partners or family members. However, very little work has empirically examined the substantive differences between familiar “friendly fraud” (E. B. Kim 2013) and unfamiliar identity theft attacks (Bradford W. Reyns 2010). A small number of studies also examine the role of family members in committing identity theft; social engineering, whereby an attacker uses persuasive conversational techniques to discover or apply a victim's credentials (Aburrous et al. 2010; Kirda and Kruegel 2006); and impersonation, whereby either an attacker pretends to be the victim in order to gain access to accounts, services or further credentials (Salem and Stolfo 2012; Bustard et al. 2014), or an attacker creates a new masquerade identity (Kemp et al. 2016; Vidal, Orozco, and Villalba 2016; He et al. 2014). In these cases, intimate knowledge of the victim can enhance the likely success and resulting damage of the attack.

The third subgroup of commission-related studies relates to behavioural factors. These studies describe the behavioural actions that might leave an individual or an organisation vulnerable to identity theft. Within this cluster, routine activities (such as regular website visits, or similar passwords across websites) (B. W. Reyns and Henson 2016; B. W. Reyns 2013; Williams 2016; Bang et al. 2012), predisposition not to report suspicious activity, and risk-seeking activities (H. Copes et al. 2010) may increase the chance of an identity theft attack. There is also evidence that routine internet access (e.g. public internet access terminals) and visits to certain types of website visited (such as online auctions and private sales) may also increase identity theft propensity (Williams 2016). Available evidence suggests that victims are still more likely to infect themselves with malware rather than via external infection (Greamo and Ghosh 2011). Within this group, there is some discussion on the role of third parties in accidentally disclosing sensitive identity data to an attacker (McKelvey 2000; Gerard, Hillison, and Pacini 2005). Such mechanisms could be via data breaches (R. E. Holtfreter and Harrington 2015; Garrison and Ncube 2011), accidentally leaving customer data in an accessible place, for instance by not securely disposing of old documents; and accidental loss, for instance through losing a laptop or USB memory stick. Among the vectors for identity theft, inadvertent disclosure remains a popular discussion point in prior literature, especially as a means to justify additional security and legal countermeasures.

Example techniques of committing identity theft are shown in Table 2. Importantly, while prior literature does describe the general function of these individual commission techniques, prior literature provides almost no analysis of the comparative popularity of these approaches, nor their relative success rates. Very little insight is provided into the relative effectiveness of these approaches, particularly among different victim groups.

Table 2 Example techniques of identity theft commission in prior literature

Method	Description	Example Citations
Credit card skimming	Credit card details including card numbers and PINs are automatically collected at the point of sale.	(Clapper 2010)
Forging documents	Documents are either modified to be false, or are solicited using false information at inception.	(Kemp et al. 2016; Baechler et al. 2011; Rudner 2008)
Data leakage	Personal data are inadvertently made available through personal devices or device features such as Bluetooth	(A. Loo 2009)
Data disposal	Personal data are inadvertently made available through incorrectly disposed devices	(Jones et al. 2009)
Data inference	Third party plugins and extensions used to access private data using an API	(Ahmadinejad and Fong 2014)
Theft of paper documents	Paper documents such as bank statements are stolen from letterboxes prior to delivery	(Mercuri 2006)
Duplicating documents	Making copies of identity tokens, such as credit cards	(Költzsch 2006)
Hacking biometrics	Forging sufficient personal identity credentials to acquire access to a biometric identity token	(Chollet et al. 2012)
Computer malware	Viruses and trojan horses can listen for user identity credentials	(Hinde 2004)
Device loss	A device holding sensitive data may be lost, thereby exposing the data	(Hinde 2004)
Credit card number generators	Software tool to generate a number that mimics credit card digits	(Hinde 2001)
Call centre staff	Call centre staff who harvest identity data from incoming calls, to on-sell later	(Moir and Weir 2009)

Types of identity theft

Studies in the literature corpus conceptualise identity theft in different ways. While the majority of studies see identity theft as an illegal use of an identity, there are a variety of different types of identity theft within this conceptualisation, and these appear to vary between studies (H. Copes et al. 2010).

Importantly, a number of studies aim to catalogue the range of identity theft types. For instance, Koops et al. (2009) develops a typology of identity crime, comprising conceptual, technical and legal categories. Jamieson et al. (2012) classify identity crimes in an online context. Broadly, we identified seven types of identity theft discussed in prior literature.

The first and most common type of identity theft occurs where an attacker seeks as great a benefit as possible. Here, the attacker obtains the identity credentials of a victim and then assumes their identity completely. Here, the attacker assumes the victim's identity as completely as possible to commit various identity-related crimes.

In the second type of identity theft, the attacker seeks to obtain one particular type of benefit and obtains only the one or two pieces of identity documentation to directly target that benefit. Examples of this approach might be gaining access to a user's social media account (using the victim's username and password login pair). Here, the attacker may discontinue the attack once they have obtained the benefit they seek.

In the third type of identity theft, the attacker uses a victim's identity documentation but only temporarily, and without any intention to benefit financially. For example, an attacker might use a victim's identity documentation to gain access to an age-restricted event such as a cinema, to receive medical treatment that they cannot otherwise obtain (Judson, Haas, and Lagu 2014), or to purchase alcohol should they be under-age (Arria et al. 2014).

In the fourth type of identity theft, the attacker creates or fabricates the necessary identity credentials, possibly supplementing these with their own identity credentials. The attacker will likely use legitimate documentation as a basis, but may create fake names, dates of birth and other individual identity tokens in order to build a convincing document. This type of identity theft is sometimes termed, “identity fraud”. Examples of this type of identity theft might include purchasing a fake passport for travel into and out of sensitive countries (Rudner 2008; Monahan 2009).

In the fifth type of identity theft, an attacker supplements real identity documentation with fabricated documentation, usually to target a particular product or service offering. For example, an attacker may possess a victim's bank statements, and then attempts to forge the victim's online banking username and password in order to gain access to their account.

In the sixth type of identity theft, one person borrows identity documents from the legitimate identity holder. This exchange may arise from a need to obtain social security benefits, or possibly in order to obtain work in a foreign country in which citizenship is not yet held (Horton 2015; Horton 2016; Clough 2015; Monahan 2009; Hovey 2009). Employers may also use this technique to mask the identity of illicit employees while still claiming employment and other social security benefits (Horton 2016).

In the seventh type of identity theft, an identity thief attacks a victim’s identity for the purposes of revenge. These attacks involve appropriating and publishing personal information or adapting intimate pictures, personal communications and social media posts in order to humiliate the victim (Henry and Powell 2016).

It is also important to note that one type of identity theft can change into another type depending on the relative success of the attack: for example, a thief may manufacture part of their victim’s identity and then use this counterfeit documentation to obtain real identity documentation for later use.

Protection and prevention

Prior literature discusses a number of mechanisms for preventing identity theft. In the main, these discussions occur at two levels – the individual and the organisational levels – with subgroups at each level.

At the individual level, such preventative discussion is often very general, prescribing protection techniques designed to prevent many identity theft attack vectors at once. These techniques usually include protecting physical and electronic personal credentials, for instance by shredding personal paperwork or encrypting personal identification data (Gilbert and Archer 2011; Milne 2003; Sharp et al. 2004; Whitson and Haggerty 2007; Perl 2003; Piquero, Cohen, and Piquero 2011); choosing secure passwords (Gilbert and Archer 2011; Bang et al. 2012); avoiding risky behaviour, including suspect links in email or SMS messages (Gilbert and Archer 2011; Lynch 2005); installing and operating up-to-date anti-virus, firewalls and spyware detection software (Eisenstein 2008; Milne 2003; Milne, Rohm, and Bahl 2004); not discussing or otherwise sharing personal information with untrusted parties (Kirda and Kruegel 2006); reviewing third party data storage credentials prior to transacting or sharing with these third parties (Galiero and Giammatteo 2009; Desmedt 2005); monitoring identity-handling agencies for irregular behaviour (Gilbert and Archer 2011; Whitson and Haggerty 2008; Acquisti and Grossklags 2005; A. D. Smith and Lias 2005). Generally, consumer education remains an important step in preventing some types of identity theft attacks (Milne 2003; Gilbert and Archer 2011; Marron 2008).

The second type of discussion at the individual level describes how to protect against specific types of identity theft attack methods. A small number of studies discuss approaches for protecting against particular types of identity theft, on the grounds that different types of identity thefts may have different causes and subsequent effects (Hoofnagle 2007; M. D. White and Fisher 2008). For example, Sullivan (2008) argues that smart cards may protect against existing account fraud because they make account transactions more complex through the use of an embedded chip that is difficult to duplicate. More studies discuss broad spectrum protections against a variety of identity thefts (Albrecht, Albrecht, and Tzafrir 2011; Sovern 2004). Many such discussions are legislative or regulatory in nature (Romanosky, Telang, and Acquisti 2011; Robert E. Holtfreter and Holtfreter 2006).Once an attack has taken place, common advice in the literature involves advising the victim to contact their relevant financial institutions (e.g. banks, insurers) to protect their details and begin the recovery process. This process often also involves contacting any government or private identity theft and credit monitoring bodies and services (such as Equifax, Experian, and TransUnion) (Eisenstein 2008). Some of these groups offer ex ante insurance policies expressly for identity theft (Piquero, Cohen, and Piquero 2011).

Behavioural defences against identity theft appear to rest on individual self-efficacy and coping mechanisms. Prior evidence suggests that the stronger an individual's ability to manage new technological and general threats, the less likely they will fall victim to an identity theft attack (Lai, Li, and Hsieh 2012; Kerstens and Jansen 2016). Interestingly, there is also voice in the literature that protecting a portion of the population against one type of identity theft might offer some 'herd' immunity to the rest of the population for some types of identity theft, on the grounds that identity thieves are dissuaded from pursuing too many unsuccessful attacks lest they be discovered (Eisenstein 2008). Incorporating behavioural modifications into daily routines may hence benefit improve protection (B. W. Reyns 2013), possibly beyond that afforded to the individual user.

A second subgroup of research examines identity theft protection and prevention at an organisational level and there is a body of work that examines identity theft prevention within organisational systems. A prevailing theme in the literature is that identity-dependent systems ought to be designed in order to preserve the identity credentials of the users and administrators of these systems (Jakobsson and Myers 2006; Gao et al. 2011; He et al. 2014). Some prior work argues that organisations that hold personal customer and employee identity information also have an ethical and legal duty of care to protect such

information (Matwyshyn 2009; Gerard, Hillison, and Pacini 2005; A. E. White 2004; Siegel 2006). While prior conceptual work has argued that increased security should reduce identity theft (Lee et al. 2012; Goode and Lacey 2011; Tow, Dell, and Venable 2010; Elson and LeClerc 2006), empirical work has found that customers' perceptions of the effectiveness and convenience security and authentication depends on the level of perceived financial risk of the transaction itself (Lee et al. 2012): this finding suggests that storage of personal data is seen as less important when transactions are not financial in nature. One body of research aims to prevent identity theft by studying the effects and benefits of information asset protection. This research aims to stop identity theft before it can occur by either preventing access to stored credentials (Burns and Roberts 2013) or by enacting processes, training and policies, usually within a single company, to more securely handle identity information (Mancilla and Moczygemba 2009). In this stream of research, much work has been conducted into various types of encryption and how they might be used to protect stored credentials: valuable reviews include Whitley et al. (2014), Yasin et al. (2012), Sabena et al. (2010) and Anand et al. (2013). This work also aims to identify operating weaknesses, particularly in software, both in the victim's computer and in an organisation's information system ecology. Prior work has found that organisational disclosures the implementation of identity theft countermeasures and management systems tend to be positively received by the market (Bose and Leung 2013; Khansa and Liginlal 2012), with newer countermeasures and earlier adoption receiving a market premium.

Another body of research examines the structure of processes used to receive, verify, process and store customer identity documentation. Such work is typically based in the health and medical literature (Brown 2012; Amori 2008), and follows changes that must be made to an individual practice in order to comply with national policy directives (such as the HIPAA Act) or large-scale system implementations (such as the eHealth Exchange) (Ahmed, Ahamad, and Jaiswal 2014). However, a number of studies in other fields, such as banking (Geeta 2011; Mohr and Fatigate 2008) also exist. Principal findings of this literature are that appropriate storage and management of customer identity data effectively prevents identity theft attacks, however almost no studies examine this effectiveness empirically. However, critical research in this stream argues that system use gives rise to unintended applications and consequences that are not foreseeable at the time of system implementation (Grijpink 2006). Further, the size of the World Wide Web itself means that it is not feasible to expect end-users to be able to monitor every use of their identity across the network (Rowe and Ciravegna 2010), and automated monitoring systems may violate privacy principles (Caloyannides 2004).Regardless of the unit of analysis, however, such discussion typically does not furnish significant analysis of the relative success rates for these protection approaches. In general, such discussion in prior literature was largely anecdotal. Naturally, any analysis of the relative success of these identity theft countermeasures would require in-depth data regarding both victims and non-victims – as a result, such research would be challenging (Lacey and Cuganesan 2004). A very small number of studies have analysed the protection effectiveness vis-a-vis specific identity theft attack methods: these exceptions include Milne (2003) who explored the effectiveness of 13 identity theft preventative activities on 61 college students and 59 non-students and found that education is the most effective general identity theft countermeasure. Burns and Roberts (2013) also studied the intention to protect personal information online, and found that perceived control over personal information mediates intention to protect. Romanosky et al. (2011) examined the introduction of state-based identity theft legislation, and found that the introduction of such laws reduced identity theft incidence by 6.1%. Holtfreter and Holtfreter (2006) also provided conceptual analysis of the effectiveness of state-based identity theft legislation.

A final component of prevention, at both the individual and the organisational levels is awareness. Awareness is a common first solution to identity theft in prior literature and is emphasized as a vital

component of identity theft defence (Al-Hamar, Dawson, and Al-Hamar 2011). Awareness describes maintaining a sense of alertness and vigilance about the possible threat posed by identity theft attacks. Atkinson et al. (2009) describe a program to increase identity theft awareness among younger technology users.

At the organisational level, awareness-building has been a key defence mechanism advocated in prior literature (Neumann 1997; Jagatic et al. 2007; Keaney 2009). Awareness, in general, contributes to heightened information security and reflects an understanding of the risks of identity theft. For example, Dinev (2006) discusses efforts by large online firms to raise awareness of identity theft. Approaches to awareness-raising in the firm might include a range of strategies, such as ongoing education programs (Arachchilage, Love, and Beznosov 2016; Butler 2007; Arachchilage and Love 2014), maintaining and enforcing security and confidentiality policies and employee training. Because identity thieves can be nimble and mobile, they are able to attack the firm from multiple angles, working to bypass controls in order to acquire useful information. Awareness at various managerial and operational levels in the firm arms employees with the mental agility to defend against social and physical compromise. Second, awareness prevents the firm from being a site of identity misuse, by helping employees identify legitimate sources and destinations for information about employees and customers. Awareness of a potential identity fraud threat contributes to a stronger culture of critically evaluating information artefacts. In turn, this heightened sensitivity helps employees better identify unauthorized requests for personal data (such as PIN and account details). Finally, awareness also protects the firm against threats from within, by signalling an environment of caution and alertness to internal attackers. In this way, awareness of identity theft can prevent the firm from being a source of information about employees, customers and internal controls for would-be offenders. Other work focuses on the role of private consumer advocacy groups such as the Anti-Phishing Working Group, Phishtank (Gupta and Pieprzyk 2011), the Identity Theft Resource Centre (Geer and Conway 2008), and the Privacy Rights Clearinghouse that rely on expert volunteers to identify and report on identity-related matters such as phishing attempts and data breaches.

Detection of identity theft

Despite a rich body of prior enquiry, comparatively little research has examined the process of detecting identity theft. In part, this gap is due to difficulties in obtaining data for research purposes (M. D. White and Fisher 2008), but also problems associated with accurately reporting identity-related crime at the individual level (Tcherni et al. 2016; Allison, Schuck, and Lersch 2005).

At the individual level, most such research focuses on the actions and responsibilities of individual customers in identifying anomalous signs of identity credential use that might indicate compromise (Whitson and Haggerty 2008). Principal findings here include extraordinary charges to credit cards or bank accounts, strange phone calls or a sudden inability to conduct normal financial transactions. To this end, identity theft detection has principally revolved around monitoring of information artefacts, such as bank statements and credit reports (Mohr and Fatigate 2008), and appropriate notification processes (such as who the affected customer should notify should they detect an anomaly).

At the organisational level, the vast majority of such research focuses on identity theft detection in the organisation's own systems. Almost no research examines organisational detection of identity theft in other organisations' systems. Even less research examines identity theft detection from the perspective of the organisation. While there is a growing literature on data breaches and associated organisational responses (Garrison and Ncube 2011), there was only a small amount of research that illustrated how

private companies and government departments (Lacey and Cuganesan 2004) detect or coordinate the detection of identity theft. While this dearth is partly due to a lack of accessible data, some argue that organisations are reluctant to participate in identity theft control because it is financially costly to report identity theft at an organisational level as the small social benefit is vastly swamped by the large reputational cost (Judson, Haas, and Lagu 2014). A further barrier to organisational reporting lies in perceived unclear legislation regarding appropriate notification requirements and procedures (Ciocchetti 2007; Shoudt 2002). Following early work citing financial disincentives for credit issuers to tackle identity theft (Sovern 2004; Geer and Conway 2008), more recent work has documented organisational participation in identity theft detection and found that such efforts can yield positive perceptions and a competitive advantage in the wider market (Bose and Leung 2013). Stronger legislation regarding organisational data management, discussed elsewhere in this review, has also been developed (Razvi 2004).

There are a variety of organisational detection techniques discussed in the literature. These techniques primarily include automated controls to identify erratic or out-of-character expenditures, financial activity or user behaviour (Rowe and Ciravegna 2010; Judson, Haas, and Lagu 2014; Feher et al. 2012; Vidal, Orozco, and Villalba 2016) on the grounds that such prior behaviour is difficult for an attacker to fabricate (Dong, Clark, and Jacob 2010; Canfora and Visaggio 2012); hunches on the part of service staff and customer agents (Lacey and Cuganesan 2004); notifications and tip-offs from customers, credit monitors, trading partners and law enforcement (Shoudt 2002; Romanosky, Telang, and Acquisti 2011). Automated detection methods are becoming increasingly popular due to the volume of identity claim traffic amid scarce investigative resources (G. Wang, Chen, and Atabakhsh 2004), and the cognitive effort required to accurately assess a person's identity given limited photographic evidence (Kemp et al. 2016). Further, it is easier to apply such automated controls across an organisation's service offerings. Analytic detection of identity theft also aims to solve identity crimes more quickly (Kemp et al. 2016): there is evidence that earlier detection of identity theft can prevent many of the negative consequences of an identity compromise, discussed elsewhere in this review (Albrecht, Albrecht, and Tzafrir 2011).

The role of industries and organisations

While the overwhelming focus of prior identity theft research has been on the individual person, some research has examined the role of organisations and industries in preventing or participating in identity theft. Typically such research discussed organisational involvement but only a small number of papers examined the organisation as the main unit of analysis (e.g. Bose and Leung 2014; Bose and Leung 2013). However, a number of relevant conceptual points regarding organisations did arise from the literature search.

Prior work has identified that some industries are at a higher risk of identity theft attack. Among these industries are banking and finance (Geeta 2011; Költzsch 2006; Mohr and Fatigate 2008), health care and medicine (Brown 2012; Amori 2008; Mancilla and Moczygemba 2009; Ahmed, Ahamad, and Jaiswal 2014), and insurance (Allison, Schuck, and Lersch 2005; Culnan and Williams 2009; Gatzlaff and McCullough 2012; Hoar 2001). These industries are typically popular because they produce identity credentials that are relied upon or can be applied in other industries, or for acquiring other identity documentation - termed "breeder documents" by Mercuri (2006) - such as applying for a loan, renting a house, or claiming social security payments. For a number of these industries at a higher risk of identity theft, steps to enact identity theft

countermeasures involve significant outlay and preparation (Gates 2010; Erickson and Howard 2007; Bose and Leung 2013).

Other industries are deemed popular among identity theft attackers because they are easy to access or have lower security barriers. These industries include education, real estate and property management, and childcare provision (Garrison and Ncube 2011). Universities, in particular, are deemed attractive because they possess large databases of staff and students, and disaggregated, sometimes poorly managed IT governance and support structures (V. R. Johnson 2005; Erickson and Howard 2007; Purkait 2012).

Organisations are typically viewed as theatres for identity theft attacks: once an attacker has sufficient identity documentation, they typically approach an organisation in order to use the documentation (K. Holtfreter et al. 2015; Holt and Turner 2012). A number of organisational types were evidenced in the literature in this capacity:

- Banks were used by the attacker to gain access to financial records and to obtain loans (both small, personal loans and larger property loans such as property mortgages).
- Insurance companies were used to establish false insurance policies for the purposes of committing insurance fraud at a later date.
- Government organisations were used to obtain or extend municipal service documentation or access to social services. These attacks typically involved government issued identity documentation such as passports, driver licences, and social security numbers.
- Telecommunications organisations were used to obtain new telephone service accounts and communications products (such as mobile phones)
- Medical providers are both sources and targets of identity theft

Importantly, identity theft attackers could also use each organisation as part of another identity theft attack, by obtaining further identity documentation (such as copies of past receipts, invoices and delivery dockets, records of previous addresses, and alternative payment mechanisms and details) (Faturoti 2015).

The role of information systems

One stream of research examines the role of systems in identity theft, typically in the commission of identity theft attacks. The three principal motivations for this work is, first, the near-ubiquity of such devices, second, the pragmatic ease with which they are used to process and store personal information and, third, the belief that such systems were not always designed with security or privacy in mind at the outset (Keaney 2009; Kahn and Roberds 2008). Identity theft is closely tied to information systems, because users require asserted identities in order to use the system (Choi, Acharya, and Gouda 2011). This principle gives rise to a number of inherent risks. First, users must be managed and communicated with, which undermines user anonymity in the system. Second, users may misconstrue user authority in the system, possibly giving rise to phishing attacks.

The two main streams of research are general information systems and mobile devices. The oldest stream of research examines general information systems and information services and the threat of identity theft. Leading research in this stream examines the extent of information system use in commercial environments, and the techniques used to preserve identity information; the threat of technical and

operating weaknesses that can be exploited by identity theft attackers; the level of trust held by customers and end-users of such information systems (Shareef and Kumar 2012); the role of standards in preserving website security against identity theft (Hinde 2001). A significant amount of work within this stream examines these concepts from the point of view of medical providers.

A prevailing explanation for the motivation to undertake identity theft is that the underlying information systems and processes are inherently complex – too complex to perfectly manage and control (Amori 2008; Roethlisberger 2011). This complexity gives rise to a sufficient number of exploitable weaknesses, especially at the junctions of such systems, that are not identifiable as the system is being designed at the outset (Grijpink 2006). That identity appears inseparable from current systems has given rise to the view that users must "cope" with identity theft weaknesses as part of their conventional use behaviours (Lai, Li, and Hsieh 2012).

Older work within this stream examined the threat of data storage to customer privacy, especially of large corporate, inter-corporate and national identity databases (E. A. Whitley and Hosein 2008). Principal threats examined by past research included the practical duration of data storage; the security threats posed by customer, staff and competitor database access (E. A. Whitley and Hosein 2008); the practical internetworking of multiple such databases, either within an organisation or among multiple organisations (Kudo et al. 2007); the development of appropriate access credentials for such databases; and the technical and operational security of the database itself (Kudo et al. 2007).

Newer research within this stream has focused more closely on online and internetworked databases. Accompanied by improvements to network technology and user access, many now argue that internetworked databases are fundamental to modern business - some work has hence explored the use of such databases in the online context, in particular identifying and understanding the vulnerabilities of online, enterprise-wide and electronic database services (A. D. Smith and Lias 2005; Elson and LeClerc 2006), and the degree to which these systems in turn make identity theft easier to commit (McCarty 2003).

A second, more recent stream, examines the role of mobile devices. Work in this stream is divided into two main areas. First, some research examines the use of mobile devices by individuals for storing personal identity information. Prominent research themes in this area include the use of mobile devices to instantiate identity for other service providers (Norouzizadeh Dezfouli et al. 2016); understanding and improving factors affecting the user's trust in their device; and the growing interconnectedness of mobile and static devices.

Identity theft recovery and outcomes

A slim stream of research focuses on the recovery process following an identity theft attack. More recent research within this stream focuses on appropriate processes for notifying potentially affected customers once their identity credentials have been compromised (Burdon, Lane, and von Nessen 2010) or accessed by an unauthorised party (Ahmed, Ahamad, and Jaiswal 2014). Discussion in this sphere typically offers prescriptive advice regarding general recovery processes. These processes include, first, notifying potentially affected parties such as banks, insurance companies, family members and, second, to contact credit protection providers in order to halt any illegitimate charges and contracts. Most such research is conceptual or anecdotal. One reason for the lack of research into recovery methods is that identity theft victims can feel very embarrassed, and they do not wish to discuss or disclose their predicament (Jones et al. 2009).

A number of outcomes arise following an identity theft attack. In early work, the two main outcomes observed were, first, significant subsequent financial hardship on the part of the victim and, second, an overwhelming effort required to regain control of their identity following the attack. A number of issues exacerbated these outcomes, including the difficulty in identifying an identity theft incident; the difficulty in compelling a third party organisation (such as a bank, insurer or telecommunications provider) to believe that the victim's real identity had been compromised, or subsequently restored; the suspicion that the identity thief was still at large, or could still cause further damage. A small amount of early work also commented on the difficulties of restoring inter-personal relationships (such as trust) following the attack.

In later work, the principal outcomes have become more varied. There has been greater emphasis on stronger corporate and individual use of credit-monitoring bodies (Romanosky, Telang, and Acquisti 2011; V. R. Johnson 2005; Sovern 2004; Vincent R. Johnson 2011; Kunkel and Richard 2010). General education, greater public awareness and more awareness programs (J. Winterdyk and Thompson 2008; Romanosky, Telang, and Acquisti 2011; Archer 2011) are also discussed in these papers.

Lawsuits and other legal action are another common outcome of an identity theft attack (Mohr and Fatigate 2008). Such lawsuits typically pit the victim against the provider or trusted keeper of the identity data (Caughey 2004; Fisher 2012; Galbraith 2012), however the fairness of such adversarial engagements is still debated (Glynn 2013). In other cases, research has discussed class action lawsuits, where the number of identity theft cases from a single breach incident is large (Clapper 2010). Organisations at the centre of identity theft attack may also undertake larger investigations to determine the source of the breach (Novak 2007).

Personal responses to identity theft attacks vary in prior literature, and they can be broadly divided into emotive, psychological and behavioural changes. Financially, victims may also experience greater difficulty in obtaining financial benefits (e.g. loans, bank accounts) until the perpetrator is caught (Cradduck and McCullagh 2008). Emotionally, identity theft victims tend to experience significant stress following the theft incident, and this stress is exacerbated if the identity theft case is not solved (Sharp et al. 2004). Common emotional responses include anxiety, embarrassment, anger and frustration (Calo 2011; Hille, Walsh, and Cleveland 2015; Sharp et al. 2004). While long-term evidence of health risks following identity theft attack is thin, Sharp et al. (2004) report that victims still experience anxiety, depression and gastrointestinal problems at 26 weeks following the attack. Overall, this prior evidence suggests that identity theft attacks are dangerous to both physical and mental health.

Identity theft risk

Prior literature conceptualises a number of risks of identity theft. Broadly, these risks can be divided into two groups, being individuals (usually consumers), and organisations (usually private companies).

With regard to individuals, risks of identity theft typically extend from the type of identity theft that has befallen the victim. For example, financial identity theft contributes to a risk of financial loss, medical identity theft contributes to risk of medical or treatment error (Amori 2008). Identity theft threats to an individual’s reputation also contribute to a risk of reputational loss (Amori 2008). Identity thefts that compromise an individual’s relation to other people or firms, such as those that breach personally sensitive data including photographs or messages (Kamal and Newman 2016), can lead to a loss of trusted relationships (He et al. 2014) which may contribute to a heightened risk of personal isolation. Such attacks may also contribute to heightened embarrassment (Jones et al. 2009), which may also dissuade victims and

affected individuals from seeking help or reporting the crime. In turn, the identity theft attack may then contribute to a perceived loss of personal freedom and an unwillingness to continue previous activities (de Bruin 2010).

With regard to organisations, the risks of identity theft appear more diverse. Most risks borne by organisations as a result of identity theft attack appear to stem initially from a loss of reputation (Amori 2008; Murray et al. 2011; Mohr and Fatigate 2008): this appears to explain why many organisations are reluctant to publicly report identity theft attacks on their customers such as large scale data breaches. It is likely that many of the conventional effects of a compromised organisational reputation come into play (e.g. Arena, Arnaboldi, and Azzone 2010; Barnett, Jermier, and Lafferty 2006). The effects of this loss of reputation can subsequently be divided into market-wide risk effects and organisation-specific risk effects.

With regard to market-wide risk effects, reputational loss can also compromise market confidence (Murray et al. 2011; R. Wright 2007)and, subsequently, market value (Bose and Leung 2014). In turn, the drop in market confidence can lead to financial loss (Amori 2008; Gerard, Hillison, and Pacini 2005). These effects can extend beyond immediate trading markets, for example, by adversely affecting perceptions of the integrity of the profession (Murray et al. 2011) and by undermining consumer confidence in online purchasing (Lynch 2005; Eisenstein 2008) and electronic payments (Schreft 2007).

With regard to organisation-specific risk effects, the reputational cost may undermine consumer trust in the organisation (Geeta 2011; Shareef and Kumar 2012; Költzsch 2006). This can affect both current and potential customers; current customers may lose confidence in the security and guardianship of the organisation (Hoofnagle 2007) and potential customers may lose confidence in the organisation's overall ability and may take their business elsewhere (Romanosky, Telang, and Acquisti 2011). The potential of this risk hence also leads to large scale expenditure on identity-preserving systems and tools across the organisation (Eisenstein 2008).

Perception

There is a small body of research that examines the generalised perception of identity theft, separate from the views of actual victims (John Winterdyk and Filipuzzi 2009). This research tends to explore the views of individuals as they relate to activities that might put them at higher risk at identity theft. The first subgroup of research examines perceptions of identity theft as they relate to electronic commerce and online transactions. Here, a principal concern is that online privacy seems to be at odds with electronic commerce transaction security on the grounds that individual identity claims must be adequately verified prior to a successful transaction (Mik 2012; Kahn and Roberds 2008): this tension has led to a significant body of work that aims to examine how individuals view identity theft risks, in both electronic commerce and elsewhere (these risks are discussed elsewhere in this review).

In general, prior work shows that individuals signal reluctance to transact online if they perceive higher risk of a subsequent identity theft, unless self-control is low in which case potential buyers downplay the risk of identity theft from an online transaction (K. Holtfreter et al. 2015). Factors such as safeguard effectiveness, trust, and self-efficacy have been positively related to online purchasing intentions (Lai, Li, and Hsieh 2012; Shareef and Kumar 2012), while the level of the perceived threat, safeguard cost, and perceived severity of a possible attack are negatively associated with online purchasing intentions (Arachchilage and Love 2013). Other research has explored the effect of a more generalised "fear" of identity theft or "privacy harm"

(Roberts, Indermaur, and Spiranovic 2013; Calo 2011), with similar results; such fear can mean users are reluctant to use a system (Mishra et al. 2014) or to transact online (Hille, Walsh, and Cleveland 2015).

The second subgroup of perception-based literature relates to a more general view of identity theft, its causes and potential outcomes. Relating expressly to the perception of identity theft, prior work seems to show that individuals are either unaware of principal identity theft vectors (Higgins et al. 2008; Marcum et al. 2015; John Winterdyk and Filipuzzi 2009; John Winterdyk and Filipuzzi 2009) or they believe that identity theft is largely a white-collar crime, committed by white collar perpetrators (H. Copes and Vieraitis 2009). A substantial amount of this prior work is based on surveys of university and high school student populations.

The implications of such perceptions are not clear. A perception that identity theft only occurs to certain members of the population could result in diminished readiness for an identity theft attack, both at an individual and an organisational level. Such perceptions may also lead to reduced or non-existent security arrangements. It is not clear why such perceptions persist. However, it is likely that portrayals of identity theft in popular media play an important role in perpetuating the perception that identity theft is infrequent and highly specialised (Morris and Longmire 2008; Turner, van Zoonen, and Harvey 2014).

Legal requirements, legislation and policy

The discussion of identity theft legislation and policy has been extensive in prior literature. On one hand, prior research into data security extended from the early 1970s: this research tended to focus on how to keep system data secure from illicit employee or competitor access, often for financial gain (Banisar and Davies 1999). To some extent, this early data security research provided both a foundation and a challenge for subsequent identity theft research: while data security was already an important topic by the advent of the World Wide Web, this new technology provided new ways of accessing, duplicating, verifying and disseminating identity credentials.

This stream provides some of the earliest research work into identity theft within the literature corpus, with studies such as Myers (1997) and Sabol (1998) describing the initial policy groundwork to protect early identity documents, including in an online context. This early research originally focused on the collection and storage of paper-based identity credentials, but later research has incorporated the electronic transaction of such documents. The dominant stream of research relating to legislation and policy relates to developing appropriate legislation at the national and corporate levels to mitigate identity theft and preserve identity credentials (Ramirez-Palafox 1998).

Much voice in the prior literature notes that most countries around the world have been slow to enact identity theft legislation. For some time, numerous countries treated identity theft attacks using older legislation designed for wire fraud, mail fraud and torts of negligence (Roethlisberger 2011; Hinde 2001). Only in the mid-2000s did countries begin enacting specific legislation to identify and control identity theft (Grijpink 2004). Hence, one stream of research describes efforts to enact identity theft policy at the national or state levels (Cradduck and McCullagh 2008; B. Wright 2004; La Fors-Owczynik 2016; Disanto 2015). Much prior work tends to focus on single legal jurisdictions. Only a small number of papers (e.g. Hiller et al. 2011; Mathews 2013) compare legislative responses across jurisdictions. The lack of legislation resulted in inconsistent law enforcement response (M. D. White and Fisher 2008; Wall 2013) and highly variable definitions of identity theft crimes (Clough 2015).

Also within this space, there is a significant amount of work in the legal services literature regarding the development, interpretation, and application of identity-related legislation. Two main types of work extend from this area. First, prior work examines the suitability of current legislative arrangements for handling identity theft cases (Roethlisberger 2011). Research in this area also examines the preparedness of individual states or nations to handle identity theft prosecution and recovery at a legislative level (B. Wright 2004; Saunders and Zucker 1999; Modisett and Lott 1999), often by way of either theoretical argument or the review of recent legal cases or laws in other jurisdictions (Myers 1997; Bale 1997). The introduction of new technologies tends to exacerbate such discussions (Wigod 1998; Gindin 1997). Second, prior work examines the conceptual meaning of 'identity' and the legislative requirements for handling how that identity is managed and handled, both on the part of individuals and organisations (Disanto 2015). Such work is often closely allied with legal treatment and conceptualisation of privacy rights and requirements (Saunders 1999; Valentine 1999; Belgum 1999). Such work often comments on the tension between reasonable privacy expectations and the need to secure financial transactions, partly because privacy was the dominant concern in early work, and not the threat of identity theft (Kang 1998; O. J. Kim 1999). In this vein, some early work also argued that individuals cannot be expected to understand or enact complete security over their full persona in either an offline or online context (Budnitz 1997; Tighe and Rosenblum 1998). Within this policy development stream, a smaller amount of research examines which identity credentials ought to be protected and which ought to be openly accessible (Caloyannides 2004). It is here that some work also aims to develop new types of identity tokens or credentials that could be effectively shared without compromising the identity of the credential holder (Jakobsson and Myers 2006; Wayman 2008).

At the national policy level, a significant amount of research has focused on the use of identity credentials to claim social security benefits and support; the use and storage of identity credentials for the purposes of voting and e-voting; and the reasonable collection and use of identity credentials for appropriate civic participation (e.g. using electoral rolls to identify swing voters) (Christensen and Schultz 2014); and notification of potentially affected individuals following an identity theft data breach (B. Wright 2004; Burdon, Lane, and von Nessen 2010). The effectiveness of this legislation is still debated, though there is evidence that such legislation has served to reduce identity theft by moderating the incidence of data breaches (Romanosky, Telang, and Acquisti 2011) or by enhancing individual citizen awareness and protective behaviours (Williams 2016). While most countries still lack explicit and direct identity theft laws, some legislation regarding the storage and use of customer data has already had significant industrial impact: much of this commentary originates from the United States. A leading example of this type of research relates to HIPAA (Gerard, Hillison, and Pacini 2005; McMahon 2004; K. M. Sullivan 2009), and its implications for medical providers in the United States. In addition to HIPAA, other national policy frameworks include the Personal Information Protection Act in Japan (Kudo et al. 2007), the Gramm-Leach-Bliley Act (McMahon 2004) and the Safeguards Rule (M. D. White and Fisher 2008). Similar academic research work focused on the European Union has been thinner (Baumer, Earp, and Poindexter 2004).

At the corporate level, a stream of research focuses on using, protecting and storing the identity credentials of its customers and employees. This research focuses on developing policy to assist customers, employees and managers to preserve identity credentials while maintaining efficiency and effectiveness of business processes. A further stream of research in this space relates to understanding and applying national or industry-side policy directives at a corporate or organisational level. For example, Judson et al. (2014) describe the implementation of identity theft control policies at Massachusetts General Hospital, and found

that while local policies had some effect in reducing identity theft, national policies were needed to support these approaches.

Gaps in Research

A number of gaps in understanding extend from this body of prior literature.

- The bulk of research into identity theft victims is based on archival data and summary statistical analysis. Data and analysis of individual victims and victim behaviour is more thin. Most such analysis occurs some time after the attack, when critical details may be lost. Very little research explicitly conceptualises victims of identity theft. Naturally, it is difficult to find participants for identity theft research, and affected victims might be too embarrassed to participate.

- While numerous papers describe the use of identity documentation in identity theft attacks in broad terms, there is little detailed work that illustrates how such documentation is used in an attack. In particular, it would be useful to know how a perpetrator assesses the usefulness of identity documentation. Very little work specifically examined how identity documents are used, and the process by which these identity documents come to be acquired by identity thieves.

- There is a lack of research into understanding the identity theft perpetrator. Consistent with information security research at large, understanding the attacker remains challenging. Motives for undertaking identity theft attacks have seen some coverage in the literature, but there is a lack of empirical work. Likewise, motive dynamics and outcomes are also deserving of further work.

- Few studies examine how different types of identity theft attack are related. It would be useful to better understand how different types of identity theft attack could give rise to sequences of identity theft outcomes and subsequent crimes.

- There has been very little prior work that explains how identity theft is practically detected. Research into detecting identity theft has typically provided only very general advice on detecting identity theft and, as noted above, almost none analyses the effectiveness of these detection techniques. Within the detection literature, most work still relies on the identification of anomalies - often on the part of an individual customer. Structured, empirically validated advice regarding detection is lacking.

- Research into organisational responses to identity theft remains reasonably thin. Deeper work in this area would likely improve resolution of identity theft cases. While financial and health-related industries appear at a higher risk, it would be useful to better understand weaknesses in other industries also. Further, only individuals are conceptualised as identity thieves: we could find no articles that examined the mechanics of organisations committing identity theft attacks. We could find very few papers that provided empirical evidence of inadvertent disclosure risk, at both the individual and organisational level, as an identity threat.

- Almost no prior work provides insight into how a third party investigative effort is used to identify that an identity theft has taken or is taking place. Very little prior work examines the role played by third parties in detecting anomalous behaviour in customer accounts, or practical examples of how automated account monitoring systems among third parties might identify irregular activity on the part of a customer.

- Even though identity credential issuing and credential use typically involve more than one stakeholder, there has been almost no prior work that examines the roles of these multiple stakeholders in detecting, controlling or reacting to identity theft or in assisting in recovering from an identity theft attack. Networked approaches to identity theft detection and management have also seen very little coverage in the literature.

- There is almost no work that examines the effectiveness of managing identity theft attacks or recovery. Most research in this space is prescriptive, but does not identify how affected individual, organisational, governmental or corporate parties could most effectively prevent or recover from an identity theft attack.

- The majority of work (more than three quarters of papers we examined) is conceptual in nature and does not apply empirical insights into theory discovery, development or testing. Only a small number of papers apply empirical support for their studies, and typically only with a small number of cases. A lack of accessible data has hampered understanding of identity theft (Tcherni et al. 2016).

- Despite much useful prior research into individual areas of focus, very few studies incorporate or synthesize multiple perspectives on the identity theft problem. This singular focus remains an important weakness because it leaves identity management processes vulnerable to attack.

- While there is some growing research into how identity information is perceived, used and stored with respect to each of the user, the device, and organisations, there is no prior research that transcends the device/user/organisation boundary. Therefore, prior understanding affords only a narrow view of identity theft commission.

- Organizational awareness is often seen as an integral defence in identity theft attacks. However, as identity theft is likely to involve information artefacts from more than one organizational source, information sharing between firms is likely also to play an important role in these defence mechanisms. While the sharing of security information has seen much prior theoretical work, there has been almost no empirical analysis of such behaviour. In addition, inter-organizational information sharing has not received much coverage in the identity theft arena, especially with regard to detection activity.

- There was evidence that there is a perception that identity theft is a highly technical and highly specialised crime. Improving such perception is likely to require careful understanding of why such perceptions exist and how they are formed. However, if these perceptions are principally influenced by popular media, then the popular media is also likely to be the best place to begin changing these views.

The Role of Communications in Prior Identity Theft Research

In this section, the report analyses prior identity theft research specifically within the context of communications and communications theory. Our goal in this section was to understand how communications had been viewed and treated in prior identity theft research, and to identify gaps in knowledge and understanding in this area.

Using the original literature corpus developed above, we extracted all papers that focused on communications issues, concepts and tools. We took a broad view of the concept of 'communications' in order to produce the most conceptually descriptive sub-corpus of literature.

In total, our sub-corpus comprised 21 journal articles. However, articles in this sub-corpus were collectively relatively new, the oldest being published in 2009. As in the previous section of the report, we read each paper in order to identify the major concepts, which we summarise below. Where appropriate, we retain the conceptual subgroups described arising from the whole literature corpus; however, with such a comparatively small collection of articles it is to be expected that not all such subgroups would be reflected in this sub-corpus. Hence we have also added new subgroups where new concepts arose within the sub-corpus.

Communications and identity theft

A common theme in the popular literature is that identity theft has become more prevalent since the advent of inexpensive and widely accessible communications and telecommunications products and services, such as the telephone, email and private messaging services (Koong et al. 2008; Ramanathan and Wechsler 2013; Banks 2015). The commercial application of these communication technologies, and the commercial services that are based on these applications, have been associated with an increase in the amount of personal data collected and stored with the use of these systems (Keaney 2009; A. A. Smith and Smith 2012; Furnell 2010). While identity crime existed long before this surge in accessible communications technology), it is worth examining the literature to specifically understand this phenomenon in prior work.

In this section, we apply a communications lens to reviewing prior literature. Specifically, in this section we focus on how identity theft has been studied with respect to communications - the transmission and receipt of identity related documentation and related concepts such as communications media and control.

One conceptual thread running through this sub-corpus of literature is that communications technology exacerbates the fallout from an identity theft attack, for a number of reasons. First, and most obviously, the communications realm also means that identity theft victims can be harmed in both the real, offline world and the virtual, online world (Fire, Goldschmidt, and Elovici 2014). For example, a victim's bank account can be targeted in the real world, and their virtual relationships and discussions can be targeted in the virtual world (He et al. 2014). Network effects, inherent in communications tools, also attract malevolent attackers as the user base grows: therefore, the more popular the communications tool, the more likely malicious users will be present (Patsakis et al. 2014).

Communications technology helps news of the attack to spread more widely and virulently: social networks in particular assist in spreading fallout from an identity theft attack as users share news of an attack, or view links, screenshots and posts regarding the attack (Patsakis et al. 2015).

Anonymity in certain communications tools, such as social networks and email, can also exacerbate the effect of an identity theft attack because the victim feels unable to identify the culprit (Schmid, Iqbal, and Fung 2015). Author attribution seems to play an important role in wresting control following an identity-related attack.

Communications tools also allow attackers to target victims without regard to geographical proximity or location. This effect means that identity crimes can be committed before local law enforcement has time to employ countermeasures, and before the local populace has the opportunity to learn and adapt (Koong et al. 2008).

Communications media and identity theft

Prior literature covered a variety of communications tools with respect to identity theft. A small amount of work specifically examined desktop computer communications and services, such as email, which is regarded as integral (and in some cases an important precursor) to newer types of identity theft attack (Schmid, Iqbal, and Fung 2015). E-mail is a common communication tool among users of a variety of ages, and it affords significant anonymity to knowledgeable users (Schmid, Iqbal, and Fung 2015). Public internet access terminals also appear to be deemed more risky forms of communications technology with respect to identity theft (Williams 2016). The progression from desktop communications devices to pervasive mobile devices also seems to have exacerbated the perceived risk of identity theft attacks (Koong et al. 2008), though there seems to be little solid evidence of the extent to which this is the case. The more frequent sharing of personally important data with such devices also may contribute to identity theft risk; these threats can include individual level threats such as sharing of address books, calendars and SMS messages, and also device and network threats such as improperly secured device features (e.g. Bluetooth) and socially engineered network attacks (A. Loo 2009).

However, we could find no papers that examined the role of communications tools prior to the popular advent of the World Wide Web. By far the largest body of modern research work relates to identity theft commission by way of the internet. In part, this observation is likely due to the contemporary rise in identity theft cases and awareness during that period. Online social networks were the most common communications media and the largest conceptual subgroup, featuring in 11 papers in this sub-corpus. Almost half of the papers in the sub-corpus focused on online social networks as a site for identity theft attacks. The popularity of social networking sites, and the frequency of use among users, has marked them as likely venues for identity theft attacks in prior literature (Norouzizadeh Dezfouli et al. 2016; Furnell and Botha 2011). In addition, the size and scale of some social networks makes identity-related attacks more cost-effective for an attacker because naïve or automated attacks might still yield useful victim outcomes (Ahmadinejad and Fong 2014).

Research in this area made several findings. First, the primary argument in this literature stream related to the level of disclosure of personal information within these social networks (Furnell 2010). Disclosed items of personal information, which could be used to establish a viable identity, include age, gender, relationship status, date of birth, email address, phone number and residential address details (Fire, Goldschmidt, and Elovici 2014; Holm 2014). Personally identifying details were also evident in multimedia uploads such as

images and video clips, permitting users to inadvertently reveal more information than they may have originally intended (Patsakis et al. 2015; Holm 2014).

Explanations for this risky sharing of personal information follow four theories. The first argument holds that privacy settings for online social networks are too complex for common users to understand and effectively manipulate. This complexity leads to inadvertent sharing on the part of the user (Patsakis et al. 2014; J. Chen et al. 2014; Furnell 2010). Further, some argue that it is in the interests of social network proprietors to encourage sharing of personal information, on the grounds that such behaviour improves site health and interactivity (Holm 2014) and market share (Patsakis et al. 2015). Varied privacy policy contents and structures between social networks may also complicate user actions and privacy decisions (Patsakis et al. 2014). The effectiveness of these privacy measures are affected by the user's own perception of the personal relevance of each measure (J. Chen et al. 2014).

The second argument holds that sharing personally identifiable information is personally satisfying to users, and this satisfaction leads users to share more information online than they might in real world (offline) situations (He et al. 2014). This satisfaction may, in part, stem from a desire to bond with other users, even wholly unknown strangers (Furnell and Botha 2011). Further, when users feel more motivated to reveal personal information, the longer it takes them to apply privacy controls to their profiles (J. Chen et al. 2014).

The third argument holds that users are reciprocally mimicking overt sharing behaviours that they identify among other users (peers, influencers and social network leaders) (Venkatanathan et al. 2014). This reciprocal behaviour leads the user to share information without always understanding the risks they face, nor appropriately understanding the level of risk safeguards put in place by other users. Sharing of personal information appears to encourage further sharing of personal information among other users (Venkatanathan et al. 2014).

The fourth argument holds that users are unaware of the risks they bear when sharing personal information, and hence cannot grasp the full costs of their disclosure (Tow, Dell, and Venable 2010). Users may also be unaware of the extent to which mobile and desktop applications share personal information with other parties, including other apps and third-party plugins (Ahmadinejad and Fong 2014; Norouzizadeh Dezfouli et al. 2016), or between social networks (Patsakis et al. 2014). This lack of awareness means that sharing personal information is not hindered (Norouzizadeh Dezfouli et al. 2016). Frequent sharing can become habitual, which can undermine the user's ability to safeguard their personal information (Williams 2016). More frequent updates also create an immediacy among users and a fear of missing out that can contribute to zealous sharing of personal information and distribution of others details (Roethlisberger 2011).

Prior literature did not identify particular user groups at heightened risk of identity theft attack, though most papers seemed to suggest that the more elaborate provision of personal information was more likely to be associated with an identity theft attack. Some work argued that child and adolescent users of social networks may be targeted or at greater risk (Fire, Goldschmidt, and Elovici 2014).

Identity theft attack and detection

Prior literature tended to conceptualise a generalised 'risk' of identity theft: most papers did not subsequently explore the mechanisms behind identity theft commission or detection.

The most common attack method described in this communications literature sub-corpus related to the interception of a victim's openly available identity information. This identity theft approach exploits a user's wish to disclose their personal information while using a particular communications medium: most such research was based on social networks (c.f. Tow, Dell, and Venable 2010), however mobile phone apps were also mentioned. The second attack vector described in prior literature involved social engineering, whereby an attacker convinces a victim to voluntarily disclose information about themselves (such as passwords or login credentials) (Ramanathan and Wechsler 2013).

Detection mechanisms received less coverage in the literature, and were primarily related to either natural detection methods and automated techniques. Natural methods depended on a victim being able to identify an attack once it had occurred (c.f. Williams 2016). To some extent, this approach depends on raising and maintaining a user's awareness of identity theft (J. Chen et al. 2014). While increased user awareness is a sought-after goal (Furnell 2010), techniques for conveying and assuring this awareness remain elusive. Despite the risks of identity theft, there is evidence that many users and consumers do not seem to take sufficient preventative measures to ameliorate these risks (Keaney 2009). Anecdotal argument holds that corporate privacy policies and government advice and information campaigns might be effective in increasing awareness among potential victims (Tow, Dell, and Venable 2010; A. Loo 2009; Keaney 2009). Others argue that communications technologies render traditional legal approaches to identity theft ineffective (Roethlisberger 2011), instead advocating for a national approach to handling identity theft attacks and remedies.

Other papers explored the role of automated detection methods. These automated techniques sometimes involve analysing text streams to determine veracity or authenticity (Schmid, Iqbal, and Fung 2015), capturing elements of prior user behaviour (also called "metadata") in order to understand current activity (Rowe and Ciravegna 2010), or comparing message properties against inventories of known fraud indicators (Ramanathan and Wechsler 2013).

Gaps in Communications Research

Communications affords attacks in two theatres: the online world and the offline world. However, the makeup of such combined attacks is not well understood, and we don't yet know how an identity theft event might move between the real world and the virtual world.

- With such a narrow sub-corpus of literature, conceptual coverage could best be described as "patchy". Papers tend not to significantly share theoretical threads or argumentative trains of thought.
- Beyond the use of the tool, few papers applied theory directly from the communications literature in order to understand the role of communications in identity theft commission, or even identity theft itself. To this end, identity theft victims are variously conceptualised as conventional users (e.g. Ahmadinejad and Fong 2014) or alternatively as customers (e.g. Ramanathan and Wechsler 2013) in prior literature, but not 'communicators'.
- While communications media are often blamed in the popular press for facilitating identity theft and other identity-related crimes, we found very few studies that explored identity theft within the communications context. It is hence reasonable to assert that contributions to knowledge would be even more important in this conceptual space.
- Journal articles in this corpus were significantly newer than those articles in the full literature corpus. Hence, it would be hence reasonable to assert that research in the area of communications is growing.
- There is almost no work that compares identity theft commission and prevalence in contexts with varying levels of communication reliance or practice: we still lack insight into how communications media, use and management affect identity theft risk, prevalence and outcomes.

Conceptual Framework

Figure 3 shows the conceptual framework that emerges from the review of prior literature. In developing this conceptual framework, we have attempted to organise the concepts raised in prior literature in order to provide a broad, bird's eye view of the principal conceptual inter-relationships discussed in prior work. In developing the conceptual framework, a number of important design decisions made. The literature review revealed that branches of theory in prior identity theft literature are typically short - studies tend to be revelatory rather than confirmatory, presenting new evidence rather than extending and strengthening prior theoretical discussion. This scientific pattern is typical of wider information security research, because most types of fraud are difficult to uncover in sufficient quantity to be able to identify and understand the underlying trends and themes. Data on these events is typically difficult to obtain and may be biased, atypical or incomplete. The opaque and sparse nature of such fraud hence makes it difficult to develop and validate theoretical relationships.

Second, while the accompanying conceptual framework suggests a number of relationships that have been identified in prior literature, a number of additional relationships are likely to exist however the literature search did not reveal evidence of these relationships in prior studies. To this end, a number of gaps must exist in prior literature in addition to those identified within the accompanying literature review itself. However, because of the sparseness of this theoretical landscape, the conceptual inter-organisation is not apparent from first principles within the literature itself. Accordingly the organisation of concepts within the conceptual framework is novel; notwithstanding the missing relationships and conceptual gaps, the organisation arises from attempting to make sense of the identity theft landscape based on interpreting the visible or logical relationships and connections evidenced in prior literature.

Attackers, victims and Identity Credentials and Documentation play an initial role in the identity theft event. In some cases, an attacker may know a victim (for instance, socially or familially) without actually engaging in identity theft. Further, the discussion of identity theft revealed identity behaviour that might be considered to be identity theft but only in certain circumstances - perhaps when consent was lacking (e.g. borrowing a sister's library card). Similarly, an attacker may have access to a victim's identity credentials without actually compromising them (for instance, if they have stolen the victim's mail, or even if they are simply living in the same house as the victim). Hence, the attacker and the victim can exist and co-exist as actors without becoming involved in an identity theft event. The victim's identity credentials are also considered actors within this context because they can exert influence independently of the credential holder: this property allows an attacker to apply a victim's credentials on their own, without the approval or involvement of the victim. That the victim is conceptually separate from their identity credentials also allows an attacker to create or synthesize credentials without the involvement of the victim, and without contact with the original credentials themselves (for example, an attacker may guess a victim's computer username/password pairing).

Perception represents how identity theft is seen. This perception affects attackers and victims - in both cases, it also subsequently affects how attackers motivate and commit identity thefts, and how victims elect to protect against and prevent such attacks. Perception affects identity credentials through their inherent value, their usefulness in committing an identity theft, and their vulnerabilities (which will vary depending on the theatres in which the identity theft takes place). In turn, these actors also influence how identity theft itself is perceived. As a result, perception directly affects available identity theft motives: if

identity theft is perceived to be a rare or harmless crime, motivations to commit identity theft may be reduced. However, if identity theft is perceived as an effective method for exacting revenge or financial benefit, then this will in turn influence the motives for choosing to commit an identity theft.

Literature discussion of motives was reasonably thin - this reflects the wider understanding of motives in the criminology literature, and the ex post facto rationalisation of criminal intent and activity. Identity theft motives are related to both the types of identity theft and the commission of identity theft. Some motives are largely opportunistic, and arise on the spur of the moment (for instance, discovering a victim's passport or driver licence on the floor). These motives hence influence the range of identity thefts of which the attacker is capable or aspirational. The attacker may conceive of a type of identity theft that is not feasible given the available opportunity, or the limits of their understanding, or their perception of possible consequences. However, the attacker may also attempt to commit an identity theft that has been influenced by their motives, or they may engage in an identity theft without an apparent motive (other than the desire to commit a crime).

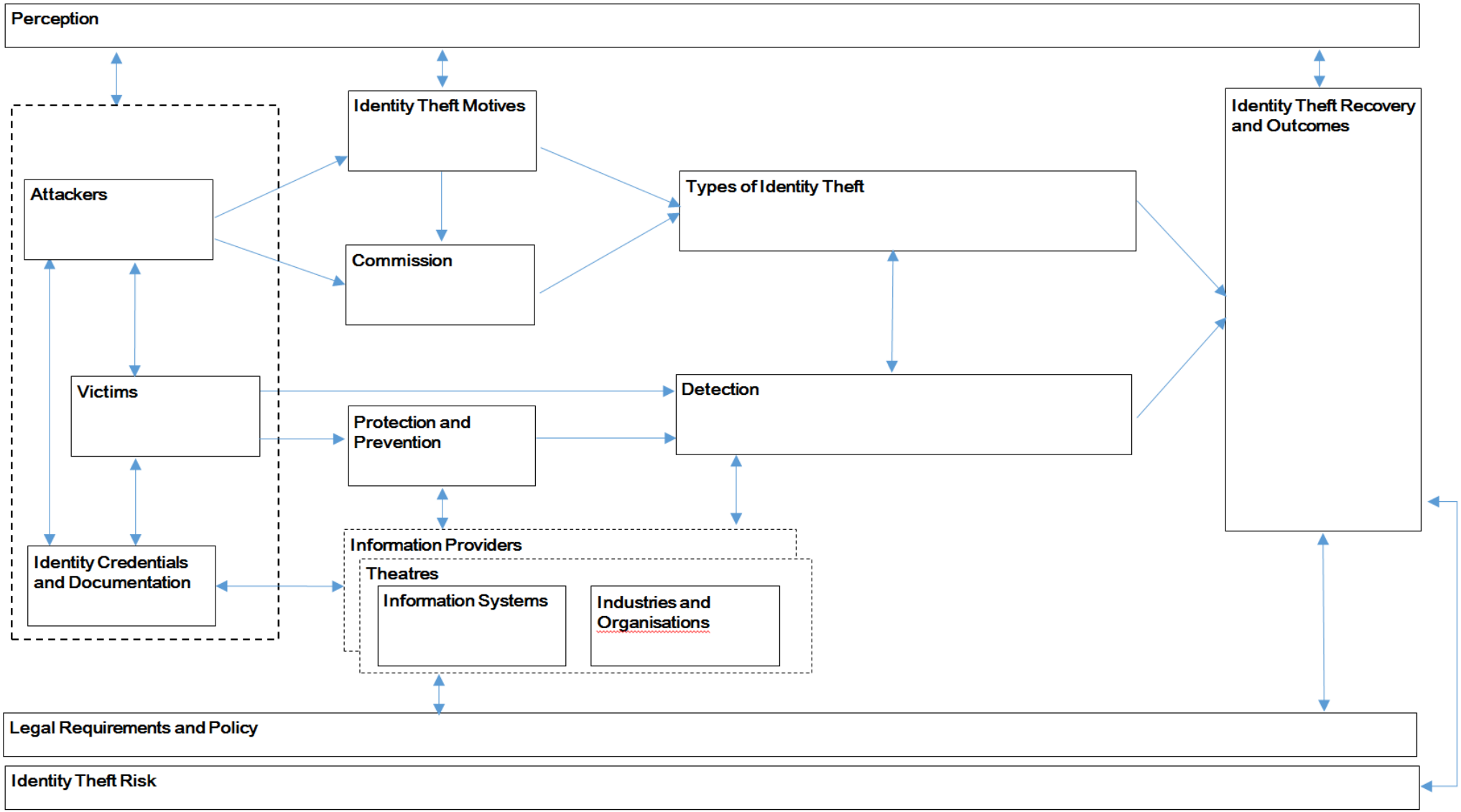
Together, motivation and commission affect the types of identity theft available to the attacker. Most prior work conceptualises identity theft in aggregate, typologizing it as a single monolithic type of fraud: as with many types of crime, it is often easier to identify and detail the antecedents and effects of crime by conceptualising the criminal activity collectively. However, individual studies do implicitly conceive of identity theft in a variety of ways: for example, in some studies, the attacker is present, and in others, the attacker is distant; in some studies, the theft is targeted and planned, and in others the attack is opportunistic. The implication of this typological variety is that identity theft itself appears to be more of a collection of identity-related compromises featuring some shared properties but also many differences: to date, these similarities and differences, and their effects, have not been well covered in the research literature.

Victims may detect identity theft directly, despite possibly attempting to prevent identity theft from occurring. Protection and prevention behaviours may directly assist the victim in discovering the identity compromise. However, these protection and prevention behaviours are also enacted by information providers in an attempt to control the compromise of their own information systems, or to be a party to an identity compromise at another site: prior literature describes a number of ways in which organisations undertake such measures, however there has been little empirical evaluation. Detection of identity theft remains a challenging concept, and much prior work suggests that most such detection occurs after an identity theft has been executed.

Identity theft takes place in a variety of theatres. Whereas the review of literature identified that organisations are seen as theatres of identity theft attack, identity compromises may occur among third parties (perhaps, through problematic identity documentation or handling), or within ad hoc information systems. The conceptual framework also categorises these theatres as information providers because they play an important role in collecting, storing, analysing or providing information to a variety of users (including private users - such as the victim or the attacker, private and public organisations, government departments and third parties).

Identity Theft recovery and outcomes reflect the events and processes that take place once an identity theft has been detected. These outcomes in turn affect the perception of identity theft on a wider basis, and the risk of identity theft more widely.

Figure 3 Conceptual Framework of Prior Identity Theft Research

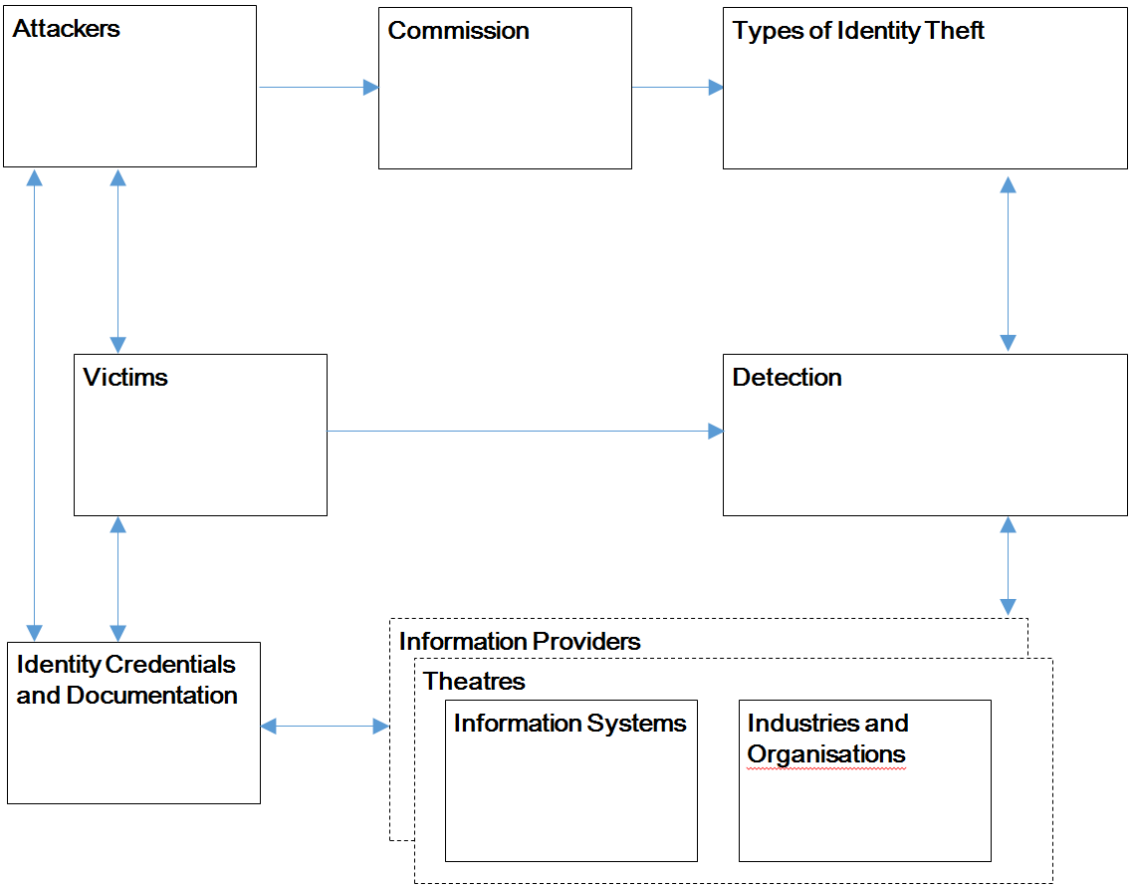


Nomological network

Accordingly, this project will abstract a subsection of the overarching conceptual framework in order to test the theoretical relationships within this group. The project's nomological network, the conceptual sub-framework to be explored in this study, is shown in Figure 4.

In sum, the project will focus on the relationship between identity theft actors (attackers, victims and identity credentials and documentation), the commission of identity theft, and the different types of identity theft that result. The project will also explore how identity theft is detected, practically by identity theft victims, and how information providers are involved. The project will also examine where identity theft crimes are committed by exploring the theatres of the crime.

Figure 4 Nomological Network of the Identity Theft Research Project



Conclusions

This document has reported on a structured literature analysis of core research papers in prior identity theft research. The document is the first report into the role of communications in identity theft in Australia. We used a three stage process to identify a set of core concepts in prior work. A list of 14 main concepts were identified, being: Conceptualising the Victim, Identity Credentials and Documentation, Conceptualising the Attacker, Identity Theft Motives, Identity Theft Commission, Types of Identity Theft, Protection and Prevention, Detection of Identity Theft, The Role of Industries and Organisations, The Role of Information Systems, Identity Theft Recovery and Outcomes, Identity Theft Risk, Perception, and Legal Requirements, Legislation and Policy. We followed this process with an analysis of prior research that specifically examined the role of communications media and technology. Three main conceptual clusters resulted from this second analysis, which were: Communications and Identity Theft, Communications Media and Identity Theft and Identity Theft Attack and Detection.

The report then presented a conceptual framework that results from the literature search, and then a nomological network of core concepts that will guide the rest of the research project.

References

Aburrous, M., M. A. Hossain, K. Dahal, and F. Thabtah. 2010. “Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies.” *Cognitive Computation* 2: 242–253.

Acquisti, Alessandro, and Ralph Gross. 2009. “Predicting Social Security Numbers from Public Data.” *Proceedings of the National Academy of Sciences* 106 (27): 10975–10980.

Acquisti, Alessandro, and Jens Grossklags. 2005. “Privacy and Rationality in Individual Decision Making.” *IEEE Security & Privacy* 2 (2005): 24–30.

Ahmadinejad, S. H., and P. W. L. Fong. 2014. “Unintended Disclosure of Information: Inference Attacks by Third-Party Extensions to Social Network Systems.” *Computers and Security* 44: 75–91.

Ahmed, M., M. Ahamad, and T. Jaiswal. 2014. “Augmenting Security and Accountability within the eHealth Exchange.” *IBM Journal of Research and Development* 58 (1): 1–11.

Albrecht, Chad, Conan Albrecht, and Shay Tzafrir. 2011. “How to Protect and Minimize Consumer Risk to Identity Theft.” *Journal of Financial Crime* 18 (4): 405–414.

Al-Hamar, M., R. Dawson, and J. Al-Hamar. 2011. “The Need for Education on Phishing: A Survey Comparison of the UK and Qatar.” *Campus-Wide Information Systems* 28: 308–319.

Allison, S. F. H., A. M. Schuck, and K. M. Lersch. 2005. “Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/Offender Characteristics.” *Journal of Criminal Justice* 33: 19–29.

Amori, G. 2008. “Preventing and Responding to Medical Identity Theft.” *Journal of Healthcare Risk Management* 28 (2): 33–42.

Anand, Darpan, Vineeta Khemchandani, and Rajendra K. Sharma. 2013. “Identity-Based Cryptography Techniques and Applications (a Review).” In *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on*, 343–348. IEEE.

Anderson, K. B. 2006. “Who Are the Victims of Identity Theft? The Effect of Demographics.” *Journal of Public Policy and Marketing* 25: 160–171.

Angell, Ian. 2008. “As I See It: Enclosing Identity.” *Identity in the Information Society* 1 (1): 23–37.

Arachchilage, N. A. G., and S. Love. 2013. “A Game Design Framework for Avoiding Phishing Attacks.” *Computers in Human Behavior* 29: 706–714.

Arachchilage, N. A. G., and S. Love. 2014. “Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective.” *Computers in Human Behavior* 38: 304–312.

Arachchilage, N. A. G., S. Love, and K. Beznosov. 2016. “Phishing Threat Avoidance Behaviour: An Empirical Investigation.” *Computers in Human Behavior* 60: 185–197.

Archer, Norm. 2011. “Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours.” *Journal of Financial Crime* 19 (1): 20–36.

Arena, Marika, Michela Arnaboldi, and Giovanni Azzone. 2010. “The Organizational Dynamics of Enterprise Risk Management.” *Accounting, Organizations and Society* 35 (7): 659–675.

Arria, A. M., K. M. Caldeira, K. B. Vincent, B. A. Bugbee, and K. E. O’Grady. 2014. “False Identification Use among College Students Increases the Risk for Alcohol Use Disorder: Results of a Longitudinal Study", Alcoholism.” *Clinical and Experimental Research* 38: 834–843.

Atkinson, S, S. M. Furnell, and A Phippen. 2009. “Securing the next Generation: Enhancing E-Safety Awareness among Young People.” *Computer Fraud & Security* 2009 (7): 13–19.

Baechler, S., E. Fivaz, O. Ribaux, and P. Margot. 2011. “False Identity Documents Profiling: A Promising Forensic Intelligence Method to Fight Identity Document Fraud.” *Revue Internationale de Criminologie et de Police Technique et Scientifique* 64: 467–480.

Bale, Robert B. 1997. “Informed Lending Decisions vs Privacy Interests in Great Britain: Technology Over the Edge of Infringement.” *Transnational Law* 10: 77–120.

Bang, Y., D.-J. Lee, Y.-S. Bae, and J.-H. Ahn. 2012. “Improving Information Security Management: An Analysis of ID-Password Usage and a New Login Vulnerability Measure.” *International Journal of Information Management* 32: 409–418.

Banisar, David, and Simon G. Davies. 1999. “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments.” *John Marshall Journal of Computer & Information Law* 18 (1): 1–113.

Banks, J. 2015. “The Heartbleed Bug: Insecurity Repackaged, Rebranded and Resold.” *Crime, Media, Culture* 11: 259–279.

Barnett, Michael L., John M. Jermier, and Barbara A. Lafferty. 2006. “Corporate Reputation: The Definitional Landscape.” *Corporate Reputation Review* 9 (1): 26–38.

Barraclough, P. A., M. Alamgir Hossain, M. A. Tahir, Graham Sexton, and Nauman Aslam. 2013. “Intelligent Phishing Detection and Protection Scheme for Online Transactions.” *Expert Systems with Applications* 40 (11): 4697–4706.

Baumer, David L., Julia B. Earp, and J. C. Poindexter. 2004. “Internet Privacy Law: A Comparison between the United States and the European Union.” *Computers & Security* 23 (5): 400–412.

Belgum, Karl D. 1999. “Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy.” *Richmond Journal of Law & Technology* 6: 1–27.

Bennison, Peter F., and Philip J. Lasher. 2005. “Data Security Issues Relating to End of Life Equipment.” *Journal of ASTM International* 2 (4): 1–7.

Berghel, Hal. 2000. “Identity Theft, Social Security Numbers, and the Web.” *Communications of the ACM* 43 (2): 17–21.

Bhargav-Spantzel, A., A. C. Squicciarini, and E. Bertino. 2006. “Establishing and Protecting Digital Identity in Federation Systems.” *Journal of Computer Security* 14: 269–300.

Bose, I., and A. C. M. Leung. 2013. “The Impact of Adoption of Identity Theft Countermeasures on Firm Value.” *Decision Support Systems* 55: 753–763.

Bose, I., and A. C. M. Leung. 2014. “Do Phishing Alerts Impact Global Corporations? A Firm Value Analysis.” *Decision Support Systems* 64: 67–78.
Brown, C. L. 2012. “Health-Care Data Protection and Biometric Authentication Policies: Comparative Culture and Technology Acceptance in China and in the United States.” *Review of Policy Research* 29: 141–159.
Budnitz, Mark E. 1997. “Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate.” *South Carolina Law Review* 49: 847–886.
Burdon, M., B. Lane, and P. von Nessen. 2010. “The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU Legal Developments.” *Computer Law and Security Review* 26: 115–129.
Burns, S., and L. Roberts. 2013. “Applying the Theory of Planned Behaviour to Predicting Online Safety Behaviour", Crime Prevention and.” *Community Safety* 15: 48–64.
Bustard, J. D., J. N. Carter, M. S. Nixon, and A. Hadid. 2014. “Measuring and Mitigating Targeted Biometric Impersonation.” *IET Biometrics* 3: 55–61.
Butler, R. 2007. “A Framework of Anti-Phishing Measures Aimed at Protecting the Online Consumer’s Identity.” *Electronic Library* 25: 517–533.
Calo, M. R. 2011. “The Boundaries of Privacy Harm.” *Indiana Law Journal* 86: 1131–1162.
Caloyannides, M. A. 2004. “Online Monitoring: Security or Social Control.” *IEEE Security and Privacy* 2: 81–83.
Canfora, G., and C. A. Visaggio. 2012. “Managing Trust in Social Networks.” *Information Security Journal* 21: 206–215.
Caughey, M. 2004. “Keeping Attorneys from Trashing Identities: Malpractice as Backstop Protection for Clients under the United States Judicial Conference’s Policy on Electronic Court Records.” *Washington Law Review* 79: 407–435.
Cavoukian, Ann. 2008. “Privacy in the Clouds.” *Identity in the Information Society* 1 (1): 89–108.
Chen, J., A. R. Kiremire, M. R. Brust, and V. V. Phoha. 2014. “Modeling Online Social Network Users’ Profile Attribute Disclosure Behavior from a Game Theoretic Perspective.” *Computer Communications* 49: 18–32.
Chen, Y., P. S. Chen, J. Hwang, L. Korba, R. Song, and G. Yee. 2005. “An Analysis of Online Gaming Crime Characteristics.” *Internet Research* 15: 246–261.
Choi, T., H. B. Acharya, and M. G. Gouda. 2011. “Is That You? Authentication in a Network without Identities.” *International Journal of Security and Networks* 6: 181–190.
Chollet, G., P. Perrot, W. Karam, C. Mokbel, S. Kanade, and D. Petrovska-Delacrétaz. 2012. “Identities, Forgeries and Disguises.” *International Journal of Information Technology and Management* 11: 138–152.
Christensen, R., and T. J. Schultz. 2014. “Identifying Election Fraud Using Orphan and Low Propensity Voters.” *American Politics Research* 42: 311–337.
Ciocchetti, Corey. 2007. “The Privacy Matrix.” *Journal of Law, Technology and Policy* 12: 245–332.

Clapper, D. L. 2010. “Stolen Data and Fraud: The Hannaford Brothers Data Breach.” *Journal of the International Academy for Case Studies* 16: 115–128.

Clough, J. 2015. “Towards a Common Identity? The Harmonisation of Identity Theft Laws.” *Journal of Financial Crime* 22 (4): 492–512.

Copes, H., K. R. Kerley, R. Huff, and J. Kane. 2010. “Differentiating Identity Theft: An Exploratory Study of Victims Using a National Victimization Survey.” *Journal of Criminal Justice* 38: 1045–1052.

Copes, H., and L. M. Vieraitis. 2009. “Understanding Identity Theft: Offenders’ Accounts of Their Lives and Crimes.” *Criminal Justice Review* 34: 329–349.

Copes, H., L. M. Vieraitis, S. M. Cardwell, and A. Vasquez. 2013. “Accounting for Identity Theft the Roles of Lifestyle and Enactment.” *Journal of Contemporary Criminal Justice* 29 (3): 351–368.

Copes, Heith, Lynne Vieraitis, and Jennifer M. Jochum. 2007. “Bridging the Gap between Research and Practice: How Neutralization Theory Can Inform Reid Interrogations of Identity Thieves.” *Journal of Criminal Justice Education* 18 (3): 444–459.

Cradduck, L., and A. McCullagh. 2008. “Identifying the Identity Thief: Is It Time for a (Smart) Australia Card.” *International Journal of Law and Information Technology* 16: 125–158.

Crompton, M. 2010. “User-Centric Identity Management: An Oxymoron or the Key to Getting Identity Management Right.” *Information Polity* 15: 291–297.

Culnan, M. J., and C. C. Williams. 2009. “How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches.” *MIS Quarterly* 33 (4): 673–687.

Damiani, Ernesto, S. De Capitani di Vimercati, and Pierangela Samarati. 2003. “Managing Multiple and Dependable Identities.” *IEEE Internet Computing* 7 (6): 29–37.

de Bruin, B. 2010. “The Liberal Value of Privacy.” *Law and Philosophy* 29: 505–534.

Deem, Debbie L. 2000. “Notes from the Field: Observations in Working with the Forgotten Victims of Personal Financial Crimes.” *Journal of Elder Abuse & Neglect* 12 (2): 33–48.

Desmedt, Y. G. 2005. “Fighting Entity Authentication Frauds by Combining Different Technologies.” *BT Technology Journal* 23 (4): 65–70.

Dilla, W. N., A. J. Harrison, B. E. Mennecke, and D. J. Janvrin. 2013. “The Assets Are Virtual but the Behavior Is Real: An Analysis of Fraud in Virtual Worlds and Its Implications for the Real World.” *Journal of Information Systems* 27: 131–158.

Dinev, Tamara. 2006. “Why Spoofing Is Serious Internet Fraud.” *Communications of the ACM* 49 (10): 76–82.

Disanto, P. F. 2015. “Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud.” *Columbia Law Review* 115: 941–982.

Dong, X., J. A. Clark, and J. L. Jacob. 2010. “Defending the Weakest Link: Phishing Websites Detection by Analysing User Behaviours.” *Telecommunication Systems* 45: 215–226.

Dowe, Erin. 2005. “Frustration Station: Attempting to Control Your Credit.” *George Mason University Civil Rights Law Journal* 16: 359–392.

Downing, C., and E. S. Geller. 2012. “A Goal-Setting and Feedback Intervention to Increase ID-Checking Behavior: An Assessment of Social Validity and Behavioral Impact.” *Journal of Organizational Behavior Management* 32: 297–306.

Downing, C., E. H. Howard, C. Goodwin, and E. S. Geller. 2016. “Preventing the Threat of Credit-Card Fraud: Factors Influencing Cashiers’ Identification-Checking Behavior.” *Journal of Prevention and Intervention in the Community* 44: 177–185.

Eisenstein, Eric M. 2008. “Identity Theft: An Exploratory Study with Implications for Marketers.” *Journal of Business Research* 61 (11): 1160–1172.

Elson, Raymond J., and Rey LeClerc. 2006. “Customer Information: Protecting the Organization’s Most Critical Asset from Misappropriation and Identity Theft.” *Journal of Information Privacy and Security* 2 (1): 3–15.

Erickson, Kris, and Philip N. Howard. 2007. “A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records.” *Journal of Computer-Mediated Communication* 12 (4): 1229–1247.

Faturoti, B. 2015. “Business Identity Theft under the UDRP and the ACPA: Is Bad Faith Always Bad for Business Advertising.” *Journal of International Commercial Law and Technology* 10: 1–12.

Feher, C., Y. Elovici, R. Moskovitch, L. Rokach, and A. Schclar. 2012. “User Identity Verification via Mouse Dynamics.” *Information Sciences* 201: 19–36.

Finn, Jerry, and Mary Banach. 2000. “Victimization Online: The Downside of Seeking Human Services for Women on the Internet.” *CyberPsychology & Behavior* 3 (5): 785–796.

Fire, M., R. Goldschmidt, and Y. Elovici. 2014. “Online Social Networks: Threats and Solutions.” *IEEE Communications Surveys and Tutorials* 16: 2019–2036.

Fisher, John A. 2012. “Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach.” *William and Mary Business Law Review* 4: 215–239.

Furnell, S. M. 2010. “Online Identity: Giving It All Away?” *Information Security Technical Report* 15: 42–46.

Furnell, S. M., and R. A. Botha. 2011. “Social Networks - Access All Areas.” *Computer Fraud and Security* 2011: 14–19.

Galbraith, Miles L. 2012. “Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information.” *American University Law Review* 62 (5): 1365–1397.

Galiero, Giulio, and Gabriele Giammatteo. 2009. “Trusting Third-Party Storage Providers for Holding Personal Information. A Context-Based Approach to Protect Identity-Related Data in Untrusted Domains.” *Identity in the Information Society* 2 (2): 99–114.

Gao, Hongyu, Jun Hu, Tuo Huang, Jingnan Wang, and Yan Chen. 2011. “Security Issues in Online Social Networks.” *IEEE Internet Computing* 15 (4): 56–63.

Garrison, C. P., and M. Ncube. 2011. “A Longitudinal Analysis of Data Breaches.” *Information Management and Computer Security* 19 (4): 216–230.

Gates, K. 2010. “The Securitization of Financial Identity and the Expansion of the Consumer Credit Industry.” *Journal of Communication Inquiry* 34: 417–431.
Gatzlaff, Kevin M., and Kathleen A. McCullough. 2012. “Implications of Privacy Breaches for Insurers.” *Journal of Insurance Regulation* 31 (1): 197–216.
Geer, D. E., and D. G. Conway. 2008. “Beware the IDs of March.” *IEEE Security and Privacy* 6 (2): 87.
Geeta, D. V. 2011. “Online Identity Theft - An Indian Perspective.” *Journal of Financial Crime* 18: 235–246.
Gerard, Gregory J., William Hillison, and Carl Pacini. 2005. “Identity Theft: The US Legal Environment and Organisations’ Related Responsibilities.” *Journal of Financial Crime* 12 (1): 33–43.
Ghazizadeh, Eghbal, Mazdak Zamani, Abolghasem Pashang, and others. 2012. “A Survey on Security Issues of Federated Identity in the Cloud Computing.” In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, 532–565. IEEE.
Gilbert, J., and N. Archer. 2011. “Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours.” *Journal of Financial Crime* 19: 20–36.
Gindin, Susan E. 1997. “Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet.” *San Diego Law Review* 34: 1153–1224.
Gleason, Maud. 2011. “Identity Theft: Doubles and Masquerades in Cassius Dio’s Contemporary History.” *Classical Antiquity* 30 (1): 33–86.
Glynn, Eric T. 2013. “The Credit Industry and Identity Theft: How to End an Enabling Relationship.” *Buffalo Law Review* 61: 215–251.
Goode, Sigi, and David Lacey. 2011. “Detecting Complex Account Fraud in the Enterprise: The Role of Technical and Non-Technical Controls.” *Decision Support Systems* 50 (4): 702–714.
Gordon, Gary R., D. J. Rebovich, Kyung-Seok Choo, and J. B. Gordon. 2007. *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*. Center for Identity Management and Information Protection, Utica College.
Gordon-Till, J. 2005. “Investigating Ordinary People: Problems and Issues.” *Business Information Review* 22: 157–165.
Grabosky, Peter. 2007. “The Internet, Technology, and Organized Crime.” *Asian Journal of Criminology* 2 (2): 145–161.
Greamo, C., and A. Ghosh. 2011. “Sandboxing and Virtualization: Modern Tools for Combating Malware.” *IEEE Security and Privacy* 9: 79–82.
Grijpink, J. 2004. “Identity Fraud as a Challenge to the Constitutional State.” *Computer Law & Security Review* 20 (1): 29–36.
Grijpink, J. 2005. “Biometrics and Identity Fraud Protection: Two Barriers to Realizing the Benefits of Biometrics - A Chain Perspective on Biometrics, and Identity Fraud Part II.” *Computer Law and Security Report* 21: 249–256.
Grijpink, J. 2006. “An Assessment Model for the Use of Biometrics.” *Computer Law and Security Report* 22: 316–319.
Gupta, Gaurav, and Josef Pieprzyk. 2011. “Socio-Technological Phishing Prevention.” *Information Security Technical Report* 16 (2): 67–73.

Halperin, Ruth, and James Backhouse. 2008. “A Roadmap for Research on Identity in the Information Society.” *Identity in the Information Society* 1 (1): 71–87.
Hansen, Marit, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, and Michael Waidner. 2004. “Privacy-Enhancing Identity Management.” *Information Security Technical Report* 9 (1): 35–44.
He, Bing-Zhe, Chien-Ming Chen, Yi-Ping Su, and Hung-Min Sun. 2014. “A Defence Scheme against Identity Theft Attack Based on Multiple Social Networks.” *Expert Systems with Applications* 41 (5): 2345–2352.
Henry, N., and A. Powell. 2016. “Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law.” *Social and Legal Studies* 25: 397–418.
Higgins, George E., Thomas “Tad” Hughes, Melissa L. Ricketts, and Scott E. Wolfe. 2008. “Identity Theft Complaints: Exploring the State-Level Correlates.” *Journal of Financial Crime* 15 (3): 295–307.
Hille, P., G. Walsh, and M. Cleveland. 2015. “Consumer Fear of Online Identity Theft: Scale Development and Validation.” *Journal of Interactive Marketing* 30: 1–19.
Hiller, Janine, Matthew S. McMullen, Wade M. Chumney, and David L. Baumer. 2011. “Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): US and EU Compared.” *Boston University Journal of Science & Technology Law* 17 (1): 1–39.
Hinde, S. 2001. “Cyberthreats: Perceptions, Reality and Protection.” *Computers and Security* 20: 364–371.
Hinde, S. 2003. “Careless about Privacy.” *Computers & Security* 22 (4): 284–288.
Hinde, S. 2004. “Confidential Data Theft and Loss: Stopping the Leaks.” *Computer Fraud & Security* 2004 (5): 5–7.
Hinde, S. 2005. “Identity Theft: Theft, Loss and Giveaways.” *Computer Fraud & Security* 2005 (5): 18–20.
Hoar, Sean B. 2001. “Identity Theft: The Crime of the New Millennium Current Developments.” *Oregon Law Review* 80: 1423–1448.
Holm, E. 2014. “Social Networking, the Catalyst for Identity Thefts in the Digital Society.” *International Journal on Advances in Life Sciences* 6: 157–166.
Holt, T. J., and M. G. Turner. 2012. “Examining Risks and Protective Factors of On-Line Identity Theft.” *Deviant Behavior* 33: 308–323.
Holtfreter, K., M. D. Reisig, T. C. Pratt, and R. E. Holtfreter. 2015. “Risky Remote Purchasing and Identity Theft Victimization among Older Internet Users.” *Psychology, Crime and Law* 21: 681–698.
Holtfreter, R. E., and A. Harrington. 2015. “Data Breach Trends in the United States.” *Journal of Financial Crime* 22: 242–260.
Holtfreter, Robert E., and Kristy Holtfreter. 2006. “Gauging the Effectiveness of US Identity Theft Legislation.” *Journal of Financial Crime* 13 (1): 56–64.
Hoofnagle, Chris Joy. 2007. “Identity Theft: Making the Known Unknowns Known.” *Harvard Journal of Law & Technology* 21 (1): 97–122.
Horton, S. B. 2015. “Identity Loan: The Moral Economy of Migrant Document Exchange in California’s Central Valley.” *American Ethnologist* 42: 55–67.

Horton, S. B. 2016. “Ghost Workers: The Implications of Governing Immigration Through Crime for Migrant Workplaces.” *Anthropology of Work Review* 37: 11–23.

Hovey, Matthew T. 2009. “Oh, I’m Sorry, Did That Identity Belong to You: How Ignorance, Ambiguity, and Identity Theft Create Opportunity for Immigration Reform in the United States Comment.” *Villanova Law Review* 54: 369–410.

Jackson, M., and J. Ligertwood. 2006. “Identity Management: Is an Identity Card the Solution for Australia.” *Prometheus (United Kingdom)* 24: 379–387.

Jackson, Shelly L. 2015. “The Vexing Problem of Defining Financial Exploitation.” *Journal of Financial Crime* 22 (1): 63–78.

Jagatic, Tom N., Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. 2007. “Social Phishing.” *Communications of the ACM* 50 (10): 94–100.

Jakobsson, Markus, and Steven Myers. 2006. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. John Wiley & Sons.

Jamieson, R., Wee Land L. P, D. Winchester, G. Stephens, A. Steel, A. Maurushat, and R. Sarre. 2012. “Addressing Identity Crime in Crime Management Information Systems: Definitions, Classification, and Empirics.” *Computer Law and Security Review* 28: 381–395.

Jiang, P., D. B. Jones, and S. Javie. 2008. “How Third-Party Certification Programs Relate to Consumer Trust in Online Transactions: An Exploratory Study.” *Psychology and Marketing* 25: 839–858.

Johnson, M. E. 2008. “Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain.” *Journal of Management Information Systems* 25 (2): 97–123.

Johnson, Margaret L. 2004. “Biometrics and the Threat to Civil Liberties.” *Computer* 37 (4): 90–92.

Johnson, V. R. 2005. “Cybersecurity, Identity Theft, and the Limits of Tort Liability.” *South Carolina Law Review* 57: 255–312.

Johnson, Vincent R. 2011. “Credit-Monitoring Damages in Cybersecurity Tort Litigation.” *George Mason Law Review* 19 (1): 113–155.

Joinson, Adam N., Carina Paine, Tom Buchanan, and Ulf-Dietrich Reips. 2006. “Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom.” *Journal of Information Science* 32 (4): 334–343.

Jones, A., G. S. Dardick, G. Davies, I. Sutherland, and C. Valli. 2009. “The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market.” *Journal of International Commercial Law and Technology* 4: 162–175.

Judson, T., M. Haas, and T. Lagu. 2014. “Medical Identity Theft: Prevention and Reconciliation Initiatives at Massachusetts General Hospital.” *Joint Commission Journal on Quality and Patient Safety* 40: 291–295.

Kahn, C. M., and W. Roberds. 2008. “Credit and Identity Theft.” *Journal of Monetary Economics* 55: 251–264.

Kamal, Mudasir, and William J. Newman. 2016. “Revenge Pornography: Mental Health Implications and Related Legislation.” *Journal of the American Academy of Psychiatry and the Law Online* 44 (3): 359–367.

Kang, Jerry. 1998. “Information Privacy in Cyberspace Transactions.” *Stanford Law Review* 50 (4): 1193–1294.

Keaney, A. 2009. “Identity Theft and Privacy - Consumer Awareness in Ireland.” *International Journal of Networking and Virtual Organisations* 6: 620–633.

Kemp, R. I., A. Caon, M. Howard, and K. R. Brooks. 2016. “Improving Unfamiliar Face Matching by Masking the External Facial Features.” *Applied Cognitive Psychology* 30: 622–627.

Kerstens, J., and J. Jansen. 2016. “The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth’s On-Line Victimization and Perpetration.” *Deviant Behavior* 37: 585–600.

Khansa, L., and D. Liginlal. 2012. “Regulatory Influence and the Imperative of Innovation in Identity and Access Management.” *Information Resources Management Journal* 25: 78–97.

Kim, Eyong B. 2013. “Information Security Awareness Status of Business College: Undergraduate Students.” *Information Security Journal: A Global Perspective* 22 (4): 171–179.

Kim, Oliver J. 1999. “The Driver’s Privacy Protection Act: On the Fast Track to National Harmony or Commercial Chaos.” *Minnesota Law Review* 84: 223–264.

Kirda, E., and C. Kruegel. 2006. “Protecting Users against Phishing Attacks.” *Computer Journal* 49: 554–561.

Kirk, David. 2014. “Identifying Identity Theft.” *Journal of Criminal Law* 78 (6): 448–450.

Költzsch, Gregor. 2006. “Innovative Methods to Enhance Transaction Security of Banking Applications.” *Journal of Business Economics and Management* 7 (4): 243–249.

Koong, K. S., L. C. Liu, S. Bai, and B. Lin. 2008. “Identity Theft in the USA: Evidence from 2002 to 2006.” *International Journal of Mobile Communications* 6: 199–216.

Koops, B.-J., R. Leenes, M. Meints, N. Van_Der_Meulen, and D.-O. Jaquet-Chiffelle. 2009. “A Typology of Identity-Related Crime.” *Information Communication and Society* 12: 1–24.

Kudo, M., Y. Araki, H. Nomiyama, S. Saito, and Y. Sohda. 2007. “Best Practices and Tools for Personal Information Compliance Management.” *IBM Systems Journal* 46: 235–253.

Kunkel, J. D., and G. Richard. 2010. “Strengthening Credit Freeze Legislation in the States: Empowering Consumers to Prevent Economic Loss from Identity Theft.” *Midwest Law Review* 23 (97): 1–51.

La Fors-Owczynik, K. 2016. “Monitoring Migrants or Making Migrants ‘Misfit’? Data Protection and Human Rights Perspectives on Dutch Identity Management Practices Regarding Migrants.” *Computer Law and Security Review* 32: 433–449.

Lacey, D., and S. Cuganesan. 2004. “The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic.” *Journal of Consumer Affairs* 38: 244–261.

Lai, F., D. Li, and C.-T. Hsieh. 2012. “Fighting Identity Theft: The Coping Perspective.” *Decision Support Systems* 52: 353–363.

Lane, G. W., and D. Z. Sui. 2010. “Geographies of Identity Theft in the U.S.: Understanding Spatial and Demographic Patterns, 2002-2006.” *GeoJournal* 75: 43–55.

Lee, J.-E. R., S. Rao, C. Nass, K. Forssell, and J. M. John. 2012. “When Do Online Shoppers Appreciate Security Enhancement Efforts? Effects of Financial Risk and Security Level on Evaluations of Customer Authentication.” *International Journal of Human Computer Studies* 70: 364–376.

Loo, A. 2009. “Technical Opinion: Security Threats of Smart Phones and Bluetooth.” *Communications of the ACM* 52: 150–152.

Loo, W. H., Paul HP Yeow, and S. C. C. Chong. 2011. “Acceptability of Multipurpose Smart National Identity Card: An Empirical Study.” *Journal of Global Information Technology Management* 14 (1): 35–58.

LoPucki, L. M. 2001. “Human Identification Theory and the Identity Theft Problem.” *Texas Law Review* 80: 89–134.

LoPucki, L. M. 2009. “Court-System Transparency.” *Iowa Law Review* 94: 481–538.

Lynch, Jennifer. 2005. “Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks.” *Berkeley Technology Law Journal* 20 (1): 259–300.

Madhusudhan, R., and R. C. Mittal. 2012. “Dynamic ID-Based Remote User Password Authentication Schemes Using Smart Cards: A Review.” *Journal of Network and Computer Applications* 35: 1235–1248.

Madsen, Paul, and Hiroki Itoh. 2009. “Challenges to Supporting Federated Assurance.” *Computer* 42 (5): 42–49.

Mancilla, D., and J. Moczygemba. 2009. “Exploring Medical Identity Theft.” *Perspectives in Health Information Management AHIMA, American Health Information Management Association* 6: 1–9.

Marcum, C. D., G. E. Higgins, M. L. Ricketts, and S. E. Wolfe. 2015. “Becoming Someone New: Identity Theft Behaviors by High School Students.” *Journal of Financial Crime* 22 (3): 318–328.

Marron, D. 2008. “Alter Reality.” *British Journal of Criminology* 48: 20–38.

Marshall, Angus M., and Brian C. Tompsett. 2005. “Identity Theft in an Online World.” *Computer Law & Security Review* 21 (2): 128–137.

Matejkovic, John E., and Karen Eilers Lahey. 2001. “Identity Theft: No Help for Consumers.” *Financial Services Review* 10 (1): 221–235.

Mathews, R. C. 2013. “International Identity Theft: How the Internet Revolutionized Identity Theft and the Approaches the World’s Nations Are Taking to Combat It.” *Florida Journal of International Law* 25: 311–330.

Matwyshyn, A. M. 2009. “CSR and the Corporate Cyborg: Ethical Corporate Information Security Practices.” *Journal of Business Ethics* 88: 579–594.

Mazzarella, William. 2004. “Culture, Globalization, Mediation.” *Annual Review of Anthropology* 33: 345–367.

McCarty, B. 2003. “Automated Identity Theft.” *IEEE Security and Privacy* 1: 89–92.

McKelvey, Brandon. 2000. “Financial Institutions’ Duty of Confidentiality to Keep Customer’s Personal Information Secure from the Threat of Identity Theft Comment.” *U.C. Davis Law Review* 34: 1077–1128.

McMahon, R. Bradley. 2004. “After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America.” *Villanova Law Review* 49: 625–660.

McPhail, Brenda, Krista Boa, Joseph Ferenbok, Karen Louise Smith, and Andrew Clement. 2009. “Identity, Privacy and Security Challenges with Ontario’s Enhanced Driver’s Licence.” In *Proceedings of the 2009 IEEE Toronto International Conference on Science and Technology for Humanity*. Toronto, Canada.

Mercuri, R. T. 2006. “Scoping Identity Theft.” *Communications of the ACM* 49: 17–21.

Mik, E. 2012. “Mistaken Identity, Identity Theft and Problems of Remote Authentication in E-Commerce.” *Computer Law and Security Review* 28: 396–402.

Milne, G. R. 2003. “How Well Do Consumers Protect Themselves from Identity Theft.” *Journal of Consumer Affairs* 37: 388–402.

Milne, G. R., A. J. Rohm, and S. Bahl. 2004. “Consumers’ Protection of Online Privacy and Identity.” *Journal of Consumer Affairs* 38: 217–232.

Mishra, A. N., P. Ketsche, J. Marton, A. Snyder, and S. McLaren. 2014. “Examining the Potential of Information Technology to Improve Public Insurance Application Processes: Enrollee Assessments from a Concurrent Mixed Method Analysis.” *Journal of the American Medical Informatics Association* 21: 1045–1052.

Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. 2013. “A Survey on Security Issues and Solutions at Different Layers of Cloud Computing.” *The Journal of Supercomputing* 63 (2): 561–592.

Modisett, Jeffrey A., and Cindy M. Lott. 1999. “Cyberlaw and E-Commerce: A State Attorney General’s Perspective.” *Northwestern University Law Review* 94 (2): 643–655.

Mohr, T. L., and R. M. Fatigate. 2008. “Compliance with the New Identity Theft Prevention Regulations.” *Banking Law Journal* 125: 518–526.

Moir, I., and G. R. S. Weir. 2009. “Contact Centres and Identity Theft.” *International Journal of Electronic Security and Digital Forensics* 2: 92–100.

Monahan, T. 2009. “Identity Theft Vulnerability: Neoliberal Governance through Crime Construction.” *Theoretical Criminology* 13: 155–176.

Morris, R. G., and D. R. Longmire. 2008. “Media Constructions of Identity Theft.” *Journal of Criminal Justice and Popular Culture* 15: 76–93.

Murray, T. L., N. C. Philipsen, E. Brice, L. Harvin, D. Hinds, and R. Warren-Dorsey. 2011. “Health Care Fraud: Stopping Nurse Imposters.” *Journal for Nurse Practitioners* 7: 753–760.

Myers, Jennifer M. 1997. “Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States.” *Case Western Reserve Journal of International Law* 29 (109): 109–147.

Neumann, Peter G. 1997. “Identity-Related Misuse.” *Communications of the ACM* 40 (7): 112–113.

Neumann, Peter G., and Lauren Weinstein. 2001. “Risks of National Identity Cards.” *Communications of the ACM* 44 (12): 176.

Ngugi, B., B. K. Kahn, and M. Tremaine. 2011. “Typing Biometrics: Impact of Human Learning on Performance Quality.” *Journal of Data and Information Quality* 2 (2): 1–21.

Norouzizadeh Dezfouli, F., A. Dehghantanha, B. Eterovic-Soric, and K.-K. R. Choo. 2016. “Investigating Social Networking Applications on Smartphones Detecting Facebook, Twitter, LinkedIn and Google Artefacts on Android and iOS Platforms.” *Australian Journal of Forensic Sciences* 48: 469–488.

Novak, C. J. 2007. “Investigative Response: After the Breach.” *Computers and Security* 26: 183–185.

Noy, David. 2009. “Neaera’s Daughter: A Case of Athenian Identity Theft?” *The Classical Quarterly* 59 (2): 398–410.

Patsakis, C., A. Zigomitros, A. Papageorgiou, and E. Galván-López. 2014. “Distributing Privacy Policies over Multimedia Content across Multiple Online Social Networks.” *Computer Networks* 75: 531–543.

Patsakis, C., A. Zigomitros, A. Papageorgiou, and A. Solanas. 2015. “Privacy and Security for Multimedia Content Shared on OSNs: Issues and Countermeasures.” *Computer Journal* 58: 518–535.

Perl, Michael W. 2003. “It’s Not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft.” *The Journal of Criminal Law and Criminology* 94 (1): 169–208.

Philpott, Andrew. 2006. “Identity Theft–dodging the Own-Goals.” *Network Security* 2006 (1): 11–13.

Phua, Clifton, Kate Smith-Miles, Vincent Lee, and Ross Gayler. 2012. “Resilient Identity Crime Detection.” *IEEE Transactions on Knowledge and Data Engineering* 24 (3): 533–546.

Piquero, N. L., M. A. Cohen, and A. R. Piquero. 2011. “How Much Is the Public Willing to Pay to Be Protected from Identity Theft.” *Justice Quarterly* 28: 437–459.

Poindexter, J. C., J. B. Earp, and D. L. Baumer. 2006. “An Experimental Economics Approach toward Quantifying Online Privacy Choices.” *Information Systems Frontiers* 8: 363–374.

Predmore, C. E., J. Rovenpor, A. R. Manduley, and T. Radin. 2007. “Shopping in an Age of Terrorism Consumers Weigh the Risks Associated with Online versus in-Store Purchases.” *Competitiveness Review* 17: 170–180.

Puckett, Carolyn. 2009. “The Story of the Social Security Number.” *Social Security Bulletin* 69 (2): 55–74.

Purkait, Swapan. 2012. “Phishing Counter Measures and Their Effectiveness – Literature Review.” *Information Management & Computer Security* 20 (5): 382–420.

Ramanathan, V., and H. Wechsler. 2013. “Phishing Detection and Impersonated Entity Discovery Using Conditional Random Field and Latent Dirichlet Allocation.” *Computers and Security* 34: 123–139.

Ramirez-Palafox, Maria. 1998. “Identity Theft on the Rise: Will the Real John Doe Please Step Forward?” *McGeorge Law Review* 29: 483–483.

Razvi, S. Kasim. 2004. “To What Extent Should State Legislatures Regulate Business Practices as a Means of Preventing Identity Theft.” *Albany Law Journal of Science and Technology* 15: 639–666.

Rege, Aunshul. 2009. “What’s Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud.” *International Journal of Cyber Criminology* 3 (2): 494–512.

Reyns, B. W. 2013. “Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses.” *Journal of Research in Crime and Delinquency* 50: 216–238.

Reyns, B. W., and B. Henson. 2016. “The Thief with a Thousand Faces and the Victim with None.” *International Journal of Offender Therapy and Comparative Criminology* 60: 1119–1139.

Reyns, Bradford W. 2010. “A Situational Crime Prevention Approach to Cyberstalking Victimization: Preventive Tactics for Internet Users and Online Place Managers.” *Crime Prevention & Community Safety* 12 (2): 99–118.

Roberts, Lynne D., David Indermaur, and Caroline Spiranovic. 2013. “Fear of Cyber-Identity Theft and Related Fraudulent Activity.” *Psychiatry, Psychology and Law* 20 (3): 315–328.

Roethlisberger, N. 2011. “Someone Is Watching: The Need for Enhanced Data Protection.” *Hastings Law Journal* 62: 1793–1838.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. “Do Data Breach Disclosure Laws Reduce Identity Theft?” *Journal of Policy Analysis and Management* 30 (2): 256–286.

Rowe, M., and F. Ciravegna. 2010. “Disambiguating Identity Web References Using Web 2.0 Data and Semantics.” *Journal of Web Semantics* 8: 125–142.

Rudner, Martin. 2008. “Misuse of Passports: Identity Fraud, the Propensity to Travel, and International Terrorism.” *Studies in Conflict & Terrorism* 31 (2): 95–110.

Sabena, Fathimath, Ali Dehghantanha, and Andrew P. Seddon. 2010. “A Review of Vulnerabilities in Identity Management Using Biometrics.” In *Future Networks, 2010. ICFN’10. Second International Conference on*, 42–49. IEEE.

Sabol, Martha A. 1998. “Identity Theft and Assumption Deterrence Act of 1998-Do Individual Victims Finally Get Their Day in Court.” *Loyola Consumer Law Review* 11 (3): 165–173.

Salem, M. B., and S. J. Stolfo. 2012. “A Comparison of One-Class Bag-of-Words User Behavior Modeling Techniques for Masquerade Detection.” *Security and Communication Networks* 5: 863–872.

Satchell, Christine, Graeme Shanks, Steve Howard, and John Murphy. 2011. “Identity Crisis: User Perspectives on Multiplicity and Control in Federated Identity Management.” *Behaviour & Information Technology* 30 (1): 51–62.

Saunders, Kurt M. 1999. “The Regulation of the Internet Encryption Technologies: Separating the Wheat from the Chaff.” *The John Marshall Journal of Information Technology & Privacy Law* 17 (3): 945–960.

Saunders, Kurt M., and Bruce Zucker. 1999. “Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act.” *International Review of Law, Computers & Technology* 13 (2): 183–192.
Schmid, M. R., F. Iqbal, and B. C. M. Fung. 2015. “E-Mail Authorship Attribution Using Customized Associative Classification.” *Digital Investigation* 14: 116–126.
Schreft, Stacey L. 2007. “Risks of Identity Theft: Can the Market Protect the Payment System?” *Economic Review-Federal Reserve Bank of Kansas City* 92 (4): 5–40.
Seda, Ludek. 2014. “Identity Theft and University Students: Do They Know, Do They Care?” *Journal of Financial Crime* 21 (4): 461–483.
Seigfried-Spellar, K. C., C. L. O’Quinn, and K. N. Treadway. 2015. “Assessing the Relationship between Autistic Traits and Cyberdeviancy in a Sample of College Students.” *Behaviour and Information Technology* 34: 533–542.
Sengupta, Shubhashis, Vikrant Kaulgud, and Vibhu Saujanya Sharma. 2011. “Cloud Computing Security–trends and Research Directions.” In *2011 IEEE World Congress on Services*, 524–531. IEEE.
Shareef, M. A., and V. Kumar. 2012. “Prevent/Control Identity Theft: Impact on Trust and Consumers’ Purchase Intention in B2C EC.” *Information Resources Management Journal* 25: 30–60.
Sharp, T., A. Shreve-Neiger, W. Fremouw, J. Kane, and S. Hutton. 2004. “Exploring the Psychological and Somatic Impact of Identity Theft.” *Journal of Forensic Sciences* 49: 131–136.
Shoudt, Erin M. 2002. “Identity Theft: Victims Cry Out for Reform.” *American University Law Review* 52 (339): 339–392.
Siegel, Kenneth M. 2006. “Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age.” *Pennsylvania State Law Review* 111 (3): 779–822.
Smedinghoff, Thomas J. 2012. “Solving the Legal Challenges of Trustworthy Online Identity.” *Computer Law & Security Review* 28 (5): 532–541.
Smith, A. A., and A. D. Smith. 2012. “CRM and Identity Theft Issues Associated with E-Ticketing of Sports and Entertainment.” *Electronic Government* 9: 1–26.
Smith, Alan D. 2005. “Identity Theft as a Threat to CRM and E-Commerce.” *Electronic Government, an International Journal* 2 (2): 219–246.
Smith, Alan D., and Allen R. Lias. 2005. “Identity Theft and E-Fraud as Critical CRM Concerns.” *International Journal of Enterprise Information Systems (IJEIS)* 1 (2): 17–36.
Smith, H. J., T. Dinev, and H. Xu. 2011. “Information Privacy Research: An Interdisciplinary Review.” *MIS Quarterly* 35 (4): 989–1016.
Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. “Information Privacy: Measuring Individuals’ Concerns about Organizational Practices.” *MIS Quarterly* 20 (2): 167–196.
Smith, Russell G., and Carolyn Budd. 2009. “Consumer Fraud in Australia: Costs, Rates and Awareness of the Risks in 2008.” *Trends & Issues in Crime and Criminal Justice*, no. 382: 1.
Solove, Daniel J. 2003. “Identity Theft, Privacy, and the Architecture of Vulnerability.” *Hastings Law Journal* 54: 1227–1276.

Southworth, Cynthia, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. 2007. “Intimate Partner Violence, Technology, and Stalking.” *Violence Against Women* 13 (8): 842–856.

Sovern, J. 2002. “The Jewel of Their Souls: Preventing Identity Theft through Loss Allocation Rules.” *University of Pittsburgh Law Review* 64: 343–406.

Sovern, J. 2004. “Stopping Identity Theft.” *Journal of Consumer Affairs* 38: 233–243.

Spitzberg, Brian H., and Gregory Hoobler. 2002. “Cyberstalking and the Technologies of Interpersonal Terrorism.” *New Media & Society* 4 (1): 71–92.

Sproule, S., and N. Archer. 2010. “Measuring Identity Theft and Identity Fraud.” *International Journal of Business Governance and Ethics* 5: 51–63.

Sullivan, C. 2008. “Privacy or Identity?” *International Journal of Intellectual Property Management* 2: 289–324.

Sullivan, Katherine M. 2009. “But Doctor, I Still Have Both Feet! Remedial Problems Faced by Victims of Medical Identity Theft.” *American Journal of Law & Medicine* 35 (4): 651–685.

Sullivan, Richard J. 2008. “Can Smart Cards Reduce Payments Fraud and Identity Theft?” *Economic Review-Federal Reserve Bank of Kansas City* 93 (3): 35–62.

Sweeney, Latanya. 2006. “Protecting Job Seekers from Identity Theft.” *IEEE Internet Computing* 10 (2): 74–78.

Sylvester, Erin Leigh. 2004. “Identity Theft: Are the Elderly Targeted?” *Connecticut Public Interest Law Journal* 3: 313–414.

Tcherni, M., A. Davies, G. Lopes, and A. Lizotte. 2016. “The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave.” *Justice Quarterly* 33: 890–911.

Tighe, Maureen A., and Emily Rosenblum. 1998. “What Do You Mean, I Filed Bankruptcy–Or How the Law Allows a Perfect Stranger to Purchase an Automatic Stay in Your Name.” *Loyola of Los Angeles Law Review* 32: 1009–1028.

Torres, Jenny, Michele Nogueira, and Guy Pujolle. 2013. “A Survey on Identity Management for the Future Network.” *IEEE Communications Surveys & Tutorials* 15 (2): 787–802.

Tow, W. N.-F. H., P. Dell, and J. Venable. 2010. “Understanding Information Disclosure Behaviour in Australian Facebook Users.” *Journal of Information Technology* 25: 126–136.

Towle, Holly K. 2004. “Identity Theft: Myths, Methods, and New Law.” *Rutgers Computer & Technology Law Journal* 30: 237–325.

Turner, G., L. van Zoonen, and J. Harvey. 2014. “Confusion, Control and Comfort: Premediating Identity Management in Film and Television.” *Information Communication and Society* 17: 986–1000.

Valentine, Debra. 1999. “About Privacy: Protecting the Consumer on the Global Information Infrastructure.” *Yale Journal of Law and Technology* 1: 4–6.

Van der Meulen, Nicole, and Bert-Jaap Koops. 2011. “The Challenge of Identity Theft in Multi-Level Governance: Towards a Coordinated Action Plan for Protecting and Empowering Victims.” In *The New Faces of Victimhood*, 159–190. Studies in Global Justice. Springer.

Veda Group. 2015. *Identity Theft in Australia: The Current Problem*. Omnibus Survey by The Leading Edge. Sydney, Australia: Veda Group.
Venkatanathan, J., V. Kostakos, E. Karapanos, and J. Gonçalves. 2014. "Online Disclosure of Personally Identifiable Information with Strangers: Effects of Public and Private Sharing." *Interacting with Computers* 26: 614–626.
Vidal, Jorge Maestre, Ana Lucila Sandoval Orozco, and Luis Javier García Villalba. 2016. "Online Masquerade Detection Resistant to Mimicry." *Expert Systems with Applications* 61: 162–180.
von Lampe, Klaus. 2008. "Mortgage Fraud and Organized Crime in Canada: Strategic Intelligence Brief." *Trends in Organized Crime* 11 (3): 301–308.
Wall, David S. 2013. "Policing Identity Crimes." *Policing and Society* 23 (4): 437–460.
Wang, Gang, Hsinchun Chen, and Homa Atabakhsh. 2004. "Criminal Identity Deception and Deception Detection in Law Enforcement." *Group Decision and Negotiation* 13 (2): 111–127.
Wang, WenJie, Yufei Yuan, and Norm Archer. 2006. "A Contextual Framework for Combating Identity Theft." *IEEE Security & Privacy* 4 (2): 30–38.
Wayman, James L. 2008. "Biometrics in Identity Management Systems." *IEEE Security & Privacy* 6 (2): 30–37.
Webster, Jane, and Richard Watson. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review." *MIS Quarterly* 26 (2): xiii–xxiii.
White, Anthony E. 2004. "The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It." *Marquette Law Review* 88: 847–866.
White, M. D., and C. Fisher. 2008. "Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts." *Criminal Justice Policy Review* 19: 3–24.
Whitley, E. A., and I. R. Hosein. 2008. "Departmental Influences on Policy Design." *Communications of the ACM* 51: 98–100.
Whitley, E. A., I. R. Hosein, I. O. Angell, and S. Davies. 2007. "Reflections on the Academic Policy Analysis Process and the UK Identity Cards Scheme." *Information Society* 23: 51–58.
Whitley, Edgar A., Uri Gal, and Annemette Kjaergaard. 2014. "Who Do You Think You Are? A Review of the Complex Interplay between Information Systems, Identification and Identity." *European Journal of Information Systems* 23 (1): 17–35.
Whitson, J, and K Haggerty. 2007. "Stolen Identities." *Criminal Justice Matters* 68 (1): 39–40.
Whitson, J., and K. Haggerty. 2008. "Identity Theft and the Care of the Virtual Self." *Economy and Society* 37: 572–594.
Wigod, Myrna L. 1998. "Privacy in Public and Private E-Mail and On-Line Systems." *Pace Law Review* 19: 95–146.
Williams, M. L. 2016. "Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level." *British Journal of Criminology* 56: 21–48.

Winterdyk, J., and N. Thompson. 2008. “Student and Non-Student Perceptions and Awareness of Identity Theft.” *Canadian Journal of Criminology and Criminal Justice* 50: 153–186.

Winterdyk, John, and Nikki Filipuzzi. 2009. “Identity Theft: Comparing Canadian and Mexican Students’ Perceptions and Awareness and Risk of Victimization.” *International Review of Victimology* 16 (3): 309–337.

Woo, J., H. J. Choi, and H. K. Kim. 2012. “An Automatic and Proactive Identity Theft Detection Model in MMORPGs.” *Applied Mathematics and Information Sciences* 6: 291–302.

Wright, Benjamin. 2004. “Internet Break-Ins: New Legal Liability.” *Computer Law & Security Review* 20 (3): 171–174.

Wright, Rosalind. 2007. “Developing Effective Tools to Manage the Risk of Damage Caused by Economically Motivated Crime Fraud.” *Journal of Financial Crime* 14 (1): 17–27.

Yasin, Shazia, Khalid Haseeb, and Rashid Jalal Qureshi. 2012. “Cryptography Based E-Commerce Security: A Review.” *International Journal of Computer Science Issues* 9 (2): 132–137.

Zhang, Lixuan, and William C. McDowell. 2009. “Am I Really at Risk? Determinants of Online Users’ Intentions to Use Strong Passwords.” *Journal of Internet Commerce* 8 (3–4): 180–197.

Zhang, Zhiyong, and Brij B. Gupta. 2016. “Social Media Security and Trustworthiness: Overview and New Direction.” *Future Generation Computer Systems* In Press: 1–12.

Authors

Sigi Goode is an associate professor of information systems in the Research School of Management at the College of Business and Economics, Australian National University (ANU). He received his Ph.D. from the Australian National University. His research interests lie in information security behaviour, services and technology adoption, policy and use. He has published papers in journals such as MIS Quarterly, Journal of Management Information Systems, European Journal of Information Systems, Decision Support Systems, Journal of Business Ethics, Information & Management, and European Journal of Operational Research. He has more than fifteen years' experience designing and managing online information platforms. Dr. Goode received the ANU Vice-Chancellor's Award for Excellence in Education in 2005, and a Carrick Institute National Award for Teaching Excellence in 2006. He is an associate editor of Information & Management and a Section Editor at the Australian Journal of Information Systems.

Identity theft and Australian telecommunications:

A structured literature review