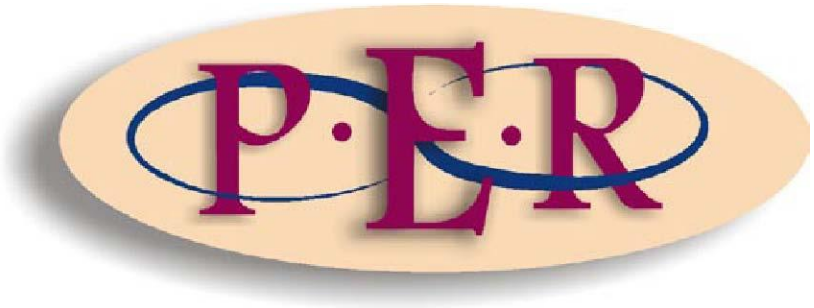
Author: F Cassim

PROTECTING PERSONAL INFORMATION IN THE ERA OF IDENTITY THEFT: JUST HOW SAFE IS OUR PERSONAL INFORMATION FROM IDENTITY THIEVES?

ISSN 1727-3781



2015 VOLUME 18 No 2

http://dx.doi.org/10.4314/pelj.v18i2.02

PROTECTING PERSONAL INFORMATION IN THE ERA OF IDENTITY THEFT: JUST HOW SAFE IS OUR PERSONAL INFORMATION FROM IDENTITY THIEVES?

F Cassim*

1 Introduction

The Internet has introduced instant and cheap communication across the globe and it has transformed commerce by making it easier for individuals to transact across a multitude of jurisdictions.[1] However, the introduction of the Internet has brought with it resultant risks and dangers and it has become vulnerable to cyber-attacks.[2] Sophisticated criminal networks are using cyberspace[3] to commit new criminal behaviours against gullible and vulnerable computer users who use the Internet to conduct their daily activities, such as sending e-mails, purchasing goods and chatting on social networking sites. The speed of the Internet also challenges the ability of law makers to regulate it effectively. The anonymity of the Internet has also facilitated cybercrimes such as identity theft.[4] This occurs when a person's personal information such as an identity document is wrongfully obtained and thereafter used to commit theft or fraud.[5] Identity theft can be committed without technical means via physical

* Fawzia Cassim. BA (UDW) LLB (UN) LLM LLD (UNISA). Associate Professor, Department of Criminal and Procedural Law, UNISA and admitted attorney and conveyancer. Email: cassif@unisa.ac.za.

1 Stevenson 2005 *Duke Law and Technology Review* 1.

2 Cyber-attacks refer to malicious attacks on information infrastructures or unauthorised access and tampering with computer systems and programmes by criminal elements. It should be noted that the term "criminals" refers to persons who engage in unlawful activities. Nuth 2008 *CLSR* 437-438; Rubin 1995 *International Journal of Law and Information Technology* 118; Goodman and Brenner 2002 *IJLIT* 144, 160.

3 The term "cyberspace" refers to a unique medium or space that has no specific geographical location but it can be available to anyone anywhere in the world who has access to the Internet (as defined in *Renor v ACLU* US 844, 851 (1997)). See Kim, Newberger and Shack 2012 *Am Crim L Rev* 485. It also refers to a virtual, borderless world where computer programmes function vis-à-vis the physical world where human beings live and function. See Cassim 2012 *PER* 381.

4 The term "cybercrime" refers to any crime carried out primarily by means of a computer on the Internet. A computer may be the "object" of a crime when there is theft of computer hardware or software, or it may be the "subject" of a crime when it is used as an instrument to commit traditional crimes such as theft, fraud or new types of criminal activity such as identity theft or child pornography. For further discussion about cybercrimes, see Cassim 2009 *PER* 36-37; Goodman and Brenner 2002 *IJLIT* 144-145; Lane and Sui 2010 *GeoJournal* 44.

5 The term "theft" is defined by Professor CR Snyman as "the unlawful and intentional appropriation of movable, corporeal property belonging to or in possession of another person with the intention to permanently deprive such person of such property", whereas the term "fraud" is defined as "the

or traditional means or by mail theft or online.[6] The identity thief uses the information *inter alia* to open credit accounts, open bank accounts, purchase merchandise and rack up debts amounting to millions of rand in the victims' names.[7] Thus, personal information is criminally obtained by identity theft, and the identity thieves use the identity-related information or data to commit unlawful activities in the victims' names.[8] The identity thieves involved operate in a multi-jurisdictional environment, which makes the tracking and prosecution of such offenders difficult and problematic.[9]

Identity theft is perceived by some to be a recent phenomenon.[10] Despite this, it is conceded that the impersonation and misuse of identity documents has existed for quite some time.[11] To illustrate this, the misuse of identity-related information was reported during the 1980s.[12] Identity thieves have used other methods such as pick-pocketing and stealing identity-related information from mail boxes to obtain and misuse people's credit and identification documents.[13] The emergence of information technology and the digital age is said to have changed the targets and methods of such offenders.[14] Indeed, the speed of technological advancement and the increased use of information technology have provided identity thieves with new, more readily-

unlawful and intentional making of misrepresentation which causes actual prejudice or which is potentially prejudicial to another person". For a detailed discussion about these terms, see Snyman *Criminal Law* 475 and 523 respectively. For a detailed discussion about identity theft, see the discussion in s 2 below.

6 Although not all cases of identity theft occur via cyberspace, significant numbers do. See Lane and Sui 2010 *GeoJournal* 43. Also see Newman *Identity Theft* 11-13, regarding the various ways in which offenders steal identities. These methods include *inter alia* the theft of wallets or purses from handbags or cars or by pick-pocketing, the theft of mail from mail boxes or the theft of personal information from dumpsters or from personal computers. It should be noted that this article will examine identity theft crimes committed by traditional conventional methods (offline) and online.

7 Perl 2003 *J Crim L & Criminology* 170,173; Newman *Identity Theft* 1.

8 The identity thieves can exploit file-sharing systems to obtain personal information and also make use of insiders who have access to stored identity-related information to obtain that information. Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html.

9 Katel 2005 *CQ Researcher* 522.

10 Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html.

11 Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html; Lynch 2005 *Berkeley Tech LJ* 262.

12 Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html.

13 Lynch 2005 *Berkeley Tech LJ* 262.

14 Grant 2006 *J Tech L & Pol'y* 3-4.

available sources of personal information.[15] Identity theft is a breach of the security which is essential to the Internet and e-commerce transactions.[16] It undermines e-commerce transactions.[17] An increase in the use of new communication technologies has thus seen a resultant increase in the commission of identity theft as vulnerabilities in computer networks are exposed and breached.[18] Identity theft disrupts the lives of thousands of people each year.[19]

Identity theft has been described by some as the "fastest growing white collar crime".[20] It cost the US economy about $ 24.7 billion during 2012; the cost to the British economy is reported to be £ 1.3 billion annually; whilst it has cost the South African economy about R1 billion a year.[21] Identity theft crimes present complex challenges for victims, law enforcement officials (police) and legislators.[22] The spate of identity thefts also highlights the need for adequate laws mandating tighter security by businesses and organisations that store and trade personal information.[23] Governments have responded to the increase in identity theft incidents by enacting laws to reduce its occurrence and severity. The article examines the effect of identity theft crimes on the personal information of individuals, the occurrence of identity thefts by traditional offline methods and in cyberspace, the impact of identity theft

---

15 The Internet is said to provide identity thieves with easier access to a large amount of personal information. Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html; Lynch 2005 *Berkeley Tech LJ* 262.

16 Sullins 2006 *Emory Int'l L Rev* 398.

17 Sullins 2006 *Emory Int'l L Rev* 398.

18 Lane and Sui 2010 *GeoJournal* 46.

19 It causes *inter alia* financial hardship and emotional suffering to victims, who spend a great amount of time and money to clear their credit records and names as a result of the identity fraud perpetuated in their names. Lane and Sui 2010 *GeoJournal* 43. For further discussion on the impact of identity theft on individuals, see the discussion in s 3 below.

20 See Hoofnagle 2007 *Harv J L & Tech* 98; Lane and Sui 2010 *GeoJournal* 43; Solove 2003 *Hastings Law Journal* 17.

21 According to a 2013 Microsoft Computing Safety Index (MCSI) involving 20 countries, including India, the United Kingdom and the United States, 15% of respondents were found to be victims of phishing attacks, 13% experienced damage to professional reputation and 9% reported that their identity had been compromised. See Microsoft Corporation 2014 http://www.Downloads/2013_MCSI_Worldwide_Results_Executive_Summary.pdf. Also see Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html; Pierson 2007 *CILW* 22; Harrell & Langton *Victims of Identity Theft* 1, 6; Ardé *Saturday Star* 3.

22 It is submitted that legislators need to introduce legislation containing *inter alia* preventative measures to address identity theft crimes.

23 It should be noted that a detailed discussion on data privacy laws and personal information laws is beyond the scope of this article. Rather, the article will address how identity thieves use the personal information of individuals to commit identity fraud or theft.

crimes on victims and the use of legislative solutions to comprehensively address identity theft. It reveals that the increase in identity theft crimes has led to the introduction of specialised legislation addressing such crimes in certain countries. The article looks at legislative solutions introduced in South Africa, the United States of America, the United Kingdom and India to combat or address such crimes. It is advocated that businesses and organisations should protect the information of individuals better. Individuals should be educated about their rights and they should become vigilant and safeguard their personal information from identity thieves.

2 Understanding how identity theft occurs[24]

In the United States, the *Identity Theft and Assumption Deterrence Act* of 1998 describes identity theft as the process whereby a person knowingly transfers or uses without lawful authority a means of identification of another person with the intent to commit or to avoid or abet any unlawful activity that constitutes a violation of federal law or a felony in terms of any state or local law.[25] Identity theft occurs when someone wrongfully obtains the personal information of another individual without their knowledge to commit theft or fraud.[26] It involves the use of another individual's personal information for nefarious purposes, such as for economic gain; to facilitate crimes such as illegal immigration, terrorism and espionage; to evade criminal sanctions or apprehension by posing as another person (criminal identity theft) or to

---

24 This section will address the definition of identity theft, the link between personal information and identity theft crimes and the different ways in which identity theft crimes occur.

25 See 18 USC s 1028(a)(7). Also see Pierson 2007 *CILW* 22; FBI 2014 http://goo.gl/TWBoep; Hoofnagle 2007 *Harv J L & Tech* 98-122; Lynch 2005 *Berkeley Tech LJ* 260; Newman *Identity Theft* 1; Lane and Sui 2010 *GeoJournal* 44. It is submitted that legislations such as the *Electronic Communications and Transactions Act* 25 of 2002 ("ECT") and the *Protection of Personal Information Act* 4 of 2013 ("POPI") may be used to address identity theft crimes in South Africa. For further discussion on the position in South African law, see s 4.1 below.

26 See FBI 2014 http://goo.gl/TWBoep; Savirimuthu 2008 *JICLT* 121 (where the writer argues that we require a better understanding of the interactions between data, devices and networks before we can introduce regulatory tools to curb practices like identity theft); Grant 2006 *J Tech L & Pol'y* 3; Perl 2003 *J Crim L & Criminology* 170, 173. It should be noted that Wi-Fi Hotspots also pose threats to the privacy of personal information. Identity theft has also been described as a type of fraud encompassing two categories, namely new account fraud where the offender opens lines of credit using the personal information of another, and account takeover where the offender uses one of the victim's existing financial accounts. For detailed information about these types of frauds, see Hoofnagle 2007 *Harv J L & Tech* 100-104.

fraudulently obtain medical services (medical identity theft).[27] Other forms of non-financial identity theft include tax identity theft, where the identity thief uses the victim's personal information to obtain government documents or benefits in the victim's name or to commit utilities fraud.[28]

These criminal acts can be committed without the assistance of technical means as well as involving the impersonation of a computer user's information online.[29] Anyone can become a victim of identity theft and one's personal information can be obtained by identity thieves through situations such as misplacing one's wallet or smartphone or from sophisticated scams such as email phishing or by criminals going through victims' trash bins or accessing information through unsecure websites.[30] The identity theft will make the victim vulnerable to crime.[31]

The identity thief obtains vital information such as identity numbers (social security numbers in the United States), medical aid numbers, addresses, birth and death certificates, passport numbers, financial account numbers such as credit card numbers, passwords, telephone numbers and biometric data (like finger prints). This information is used *inter alia* to open bank accounts, obtain credit and purchase merchandise and services in the victims' names. Thus the identity thief can rack up huge debts in the victims' names.[32] Information such as the date of birth and address

---

27 This demonstrates that the "gain" sought by identity thieves encompasses more than mere economic or financial gain. For a detailed discussion about the different types of identity theft, see Smith 2014 http://goo.gl/SvDuXn; Keenan 2005-2006 *Shidler J L Com & Tech* 2-3; Solove 2003 *Hastings Law Journal* 16-19; Gercke 2011 http://www.itu.int/ITU- D/cyb/cybersecurity/ legislation/html; Newman *Identity Theft* 14-19. Also see Action Fraud 2014 http://www.actionfraud.police.uk.

28 See Perl 2003 *J Crim L & Criminology* 177-181 for a detailed discussion about these types of identity theft.

29 Criminals may search for personal or confidential information in trash or garbage bins at malls or offices. These thieves resort to traditional means rather than electronic means to obtain personal information. Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html.

30 Burquest and Wilkinson 2013 *Tax Adviser* 223. Also see Grant 2006 *J Tech L & Pol'y* 3-4; Katel 2005 *CQ Researcher* 524. Regarding additional methods as to how identity thieves may obtain a victim's personal information see Perl 2003 *J Crim L & Criminology* 173-175.

31 Newman *Identity Theft* 13-14.

32 This is known as financial identity theft. See Nuth 2008 *CLSR* 439; Perl 2003 *J Crim L & Criminology* 176-177.

can assist the offender to avoid verification processes such as the use of biometric information as an identification tool.[33]

Identity theft is also considered to incorporate phishing.[34] Phishing refers to the use of emails to trick victims into disclosing their personal and financial information.[35] Phishers use information obtained via their scams to commit identity theft and fraud.[36] Identity thieves have also diverted their attention to social networking sites and they may eavesdrop into communications conducted over networks.[37]

3 The impact of identity theft

Many individuals and companies have fallen victim to identity theft.[38] It causes financial loss to consumers, creditors, financial institutions and the economy as a whole.[39] It has been reported by the credit bureau Compuscan that identity theft costs the South African economy about R1 billion a year.[40] According to the US Federal Trade Commission, identity theft is a major subject of consumer complaints.[41] Identity theft cost the American economy about $24.7 billion during 2012, whilst it costs the British economy about £1.3 billion every year.[42] The time and money spent responding

---

33 Biometric information refers for instance to the use of finger prints as identification tools. These tools are said to be costly to use; hence identity theft incidents have become easier for identity thieves to commit where these identification tools are not used. Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html.

34 The Anti-Phishing Working Group ("APWG") also regards phishing as a form of online identity theft. Lynch 2005 *Berkeley Tech LJ* 265, 278-284; Nuth 2008 *CLSR* 439; Sullins 2006 *Emory Int'l L Rev* 368, 397.

35 Nuth 2008 *CLSR* 439; Sullins 2006 *Emory Int'l L Rev* 397-398.

36 For more information on phishing, see *inter alia* Lynch 2005 *Berkeley Tech LJ* 259; Savirimuthu 2008 *JICLT* 121; Black 2005 *JLIS* 74; Almahroos 2007-2008 *J L & Pol'y* 596; Cherry 2005-2006 *J L & Pol'y* 593.

37 Savirimuthu 2008 *JICLT* 126. Regarding other types of identity theft, see Newman *Identity Theft* 14-19.

38 Indeed, there are said to be two types of victims of identity theft: the actual people whose identities are stolen and the companies who possess the information when it is stolen. Grant 2006 *J Tech L & Pol'y* 5.

39 Identity theft causes emotional upheaval to victims and it has a direct impact on the finances of victims. The victims find it difficult to obtain loans, credit cards or mortgage bonds from financial institutions as a result of the identity theft incident until the matter has been resolved. See Hoofnagle 2007 *Harv J L & Tech* 98.

40 Ardé *Saturday Star* 3.

41 Newman *Identity Theft* 4.

42 Pierson 2007 *CILW* 22; Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html. The worldwide annual cost of identity theft and phishing is said to be $5 billion and the cost of repairing damage to people's reputation online is $6 billion. See Waugh 2014

to an identity theft incident is also extensive.[43] Financial institutions pass on the losses to consumers with the result that consumers end up paying higher interest rates.[44] Identity theft has the potential to break down traditional spatial barriers for crime and it involves multiple jurisdictions.[45] The increase in identity theft offences following hurricane Katrina in the United States demonstrates that the location of a major catastrophe and changes in human conditions can directly affect crime patterns.[46]

Losses suffered by victims encompass pain and suffering, psychological damage, financial losses, harassment from debt collectors and creditors, the rejection of applications for loans and mortgage bonds from financial institutions, damage to reputations and possible arrest for the identity thief's other crimes.[47] Victims suffer harm to their reputations as a result of criminal activities committed in their names. They don't typically discover the crime until after some time has passed, and it may take the victims a long time to clear their names and credit history.[48] They are usually uncertain as to how their personal data was stolen or who stole their personal information. The fraud usually goes undetected as the victims rarely report the crime to law enforcement agencies.[49]

Financial institutions are also reluctant to report such crimes as they are worried about bad publicity, the loss of their reputations and the loss of public confidence.[50] This reluctance is disconcerting as authorities and law enforcement agencies should be timeously informed about such attacks on company IT systems in order to aid their understanding of and preparation against criminal activities on the Internet. The difficulty regarding proper forms of online identification has also compounded the verification of users over the Internet. Sophisticated identification tools such as

---

http://www.welivesecurity.com/2014/02/12; Microsoft Corporation 2014 http://www.Downloads/2013_MCSI_Worldwide_Results_Executive_Summary.pdf.

43 Pierson 2007 *CILW* 23.

44 Solove 2003 *Hastings Law Journal* 19.

45 Lane and Sui 2010 *GeoJournal* 44.

46 Lane and Sui 2010 *GeoJournal* 53.

47 Newman *Identity Theft* 4-5; Lynch 2005 *Berkeley Tech LJ* 263-264.

48 Lynch 2005 *Berkeley Tech LJ* 264.

49 Hoofnagle 2007 *Harv J L & Tech* 105. For more information on the inadequacy of law enforcement agencies to attend to the problem of identity theft, see Hoofnagle 2007 *Harv J L & Tech* 106-108.

50 Hoofnagle 2007 *Harv J L & Tech* 107.

biometric information are considered to be costly and are not widely used.[51] The availability of tools to commit cybercrime has also made identity theft easy and profitable for offenders.[52]

4 Legislation addressing identity theft

The increase in identity theft crimes has led to the promulgation of specialised legislation to address the challenges they pose. Adequate preventative measures are needed to respond to identity theft crimes.[53] The following section will examine the introduction of legislative solutions in selected jurisdictions to address the increase in incidents of such fraud and the theft of personal information.

4.1 South Africa

There has been an increase in identity theft crimes in South Africa with identity thieves using stolen identities to open credit accounts, run up debts and claim false tax refunds from the South African Revenue Service ("SARS").[54] It has been recently reported that retailers, banks, cell phone stores and travel agents are carelessly discarding clients' sensitive personal information in trash bins at shopping malls.[55] This constitutes "easy pickings" for identity thieves who can use the information to open bank accounts, buy goods, illegally apply for credit and access medical aids in their victims' names.

The South African Banking Risk Information Centre ("SABRIC") has warned South African consumers against a new scam that is designed to trick people into compromising their personal information.[56] According to SABRIC, the scam targets home computer users and masquerades as legitimate telephonic calls from reputable

51 Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html.
52 Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html.
53 Hoofnagle 2007 *Harv J L & Tech* 122.
54 Thakali *Saturday Star* 7; Ardé *Saturday Star* 3; SARS 2014 http://www.sars.gov.za/TargTaxCrime/Pages/Identity.Fraud.aspx.
55 Thakali *Saturday Star* 7.
56 Anon 2013 http://www.elaw@legalbrief.co.za. It should be noted that SABRIC is a wholly owned subsidiary of the Banking Association of South Africa funded by the major banks in South Africa. It was established in 2002 to address bank-related crime through effective public private partnerships. For further information, see SABRIC 2014 https://www.sabric.co.za.

computer stores.[57] The South African Department of Home Affairs is presently implementing the Home Affairs National Identification System ("HANIS"), which aims to replace the current paper system with a digital database and thus address identity theft committed by the stealing of identity documents.[58] A partnership has also been established between SABRIC and the Department of Home Affairs to grant banks access to HANIS for the verification of the identity of prospective and current bank customers. This is commendable.

In South Africa, identity theft is prosecuted in terms of the common law.[59] A person guilty of identity theft may be found guilty of fraud, forgery and uttering a forged document, and this depends on the circumstances of each case. Certain minimum sentences are imposed in terms of the Criminal Law Amendment Act for the offences of fraud, forgery and uttering a forged document, ranging from imprisonment for 15 years to 25 years depending on the amount involved and the type of offender.[60] The Southern African Fraud Prevention Service ("SAFPS") is tasked with combating fraud in society by protecting consumers against impersonation and identity theft.[61]

The Cybersecurity Policy Framework was passed by the South African Cabinet on 11 March 2012. The aims are *inter alia* to promote cyber security online; to co-ordinate government actions on cyber security and to ensure co-operation between the government, the private sector and civil society in addressing cyber threats; to examine areas of responsibility for government departments and to task the State Security Agency with overall accountability for the development and implementation of cyber security measures.[62]

---

57 The victims are advised that their systems are faulty or compromised and that they need urgent remedial action. They are tricked into divulging their personal information and into unknowingly installing or accepting malware on their computers during the telephonic conversation. Anon 2013 http://www.fin24.com/Economy/Beware-new-software-identity-theft-scam-20130408.

58 See Smith 2014 http://goo.gl/SvDuXn.

59 Smith 2014 Smith 2014 http://goo.gl/SvDuXn. However, legislations such as the *Protection of Personal Information Act* 4 of 2013 and the *Electronic Communications and Transactions Act* 25 of 2002 may be used to address identity theft crimes in South Africa. For further discussion regarding such legislations, see ss 4.1.1 and 4.1.2 below.

60 See s 51 read with Part 11 of Schedule 2 of the *Criminal Law Amendment Act* 105 of 1997.

61 For more information, see the website: SAFPS 2014 http://www.safps.org.za.

62 The policy has yet to be fully implemented. A need also arises to develop more robust Computer Emergency Readiness Teams (CERTs) to respond to cyber incidents, to provide technical

It is submitted that the following legislations may be used to stop the abuse of personal information in South Africa and to prevent identity theft.

4.1.1 Protection of Personal Information Act 4 of 2013 ("POPI")

POPI seeks to give effect to section 14 of the *Constitution of the Republic of South Africa*, 1996 ("*Constitution*"). Section 14 provides that everyone has a right to privacy.[63] The preamble to POPI provides that the right to privacy includes the right to protection against the unlawful collection, retention, dissemination and use of personal information. POPI was signed into law during November 2013. It promotes *inter alia* the protection of personal information processed by private and public bodies; provides for the protection of the rights of persons regarding unsolicited electronic communications; provides for the introduction of certain conditions so as to establish minimum requirements for the processing of personal information and regulates the flow of personal information across the borders of South Africa.[64] The purpose of POPI is *inter alia* to regulate the manner in which personal information may be processed by establishing conditions prescribing minimum standards for the lawful processing of personal information.[65] Key terms are defined in chapter 1 of POPI. It defines personal information as "information relating to an identifiable, living natural person and where applicable, an identifiable, existing juristic person".[66] The term "data subject" is defined in POPI as the "person to whom personal information relates".[67] It should be noted that the term "processing" refers to any operation or activity or set of operations, whether or not it takes place by automatic means, relating

---

assistance to businesses affected by cybercrime and to avert cyber threats. See, further, Tamarkin 2014 http://goo.gl/pmLxZb; Jones 2014 http://goo.gl/MCVT4c.

63 This right is subject to the limitation clause in s 36 of the *Constitution*.

64 See *inter alia* chs 3, 9 and 11 of POPI. Ch 3 regulates the conditions for the lawful processing of personal information; ch 9 regulates transborder information flows, whilst ch 11 regulates offences, penalties and administrative fines. It should be noted that s 72 specifically regulates the transfer of personal information outside South Africa.

65 See s 2(b) of POPI.

66 It should be noted that the term "electronic communications" refers to any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient. See ch 1 of POPI.

67 It should be noted that the term "data" is not defined in POPI. It is submitted that the term "personal data" may refer to electronic representations of personal information. A "data collector" could refer to the "operator" who processes the personal information of the natural or juristic person in terms of a contract or mandate. For further information regarding definitions of key terms, see ch 1 of POPI.

to personal information, and it includes *inter alia* the collection, receipt, recording, storage, retrieval or use of information, whilst the term "record" refers to any recorded information regardless of the form or medium.[68] Thus, it may be argued that POPI (which protects personal information) may be used to address identity theft, which involves *inter alia* the perpetration of fraud whereby the identity thief uses the personal information of the individual to open bank accounts, to obtain credit, to purchase goods and services in the individual's name or to achieve nefarious dealings such as illegal immigration, espionage or terrorism.

The Act places obligations on companies to process personal information responsibly.[69] Such companies also cannot collect personal information without the prior consent of the individuals and they cannot divulge or sell personal information to other companies for marketing purposes.[70] POPI requires data collectors to register with the Information Protection Regulator.[71] Individuals can now request companies to provide information free of charge as to whether or not they hold the personal data of the individual and to whom such data was disclosed.[72] Companies will have to implement appropriate, reasonable and organisational measures to prevent the unauthorised use of personal information and invest in new technologies such as encryption and access control.[73] Section 21 places an obligation on companies to notify the individual of any unauthorised use or disclosure of personal information to afford the individual an opportunity to take protective measures.[74] Companies have to appoint Information Protection Officers to ensure compliance with the provisions of

---

68 It is submitted that the term "processing" may incorporate the use and storage of personal information by traditional or conventional means (such as written format) and electronic means. See ch 1 of POPI for a detailed definition about key terms.

69 See s 19 of POPI. Also see Thakali *Saturday Star* 7. It should be noted that s 22 addresses security compromises.

70 See s 69 of POPI.

71 The Information Protection Regulator refers to a juristic person established in s 39 of POPI. S 40 sets out the duties and functions of the Regulator, which include *inter alia* providing education on the Act to private or public bodies and data subjects, monitoring and enforcing compliance by private and public bodies regarding the Act, and handling complaints about alleged violations of the Act.

72 See s 23 of POPI. Also see Luck 2014 *De Rebus* 45-46 for a discussion about POPI's key features.

73 See s 19 of POPI.

74 To illustrate this, the theft of an employee's computer must be disclosed to every person whose data is at risk. Also see Luck 2014 *De Rebus* 46.

the Act.[75] POPI allows for fines of up to R10 million or imprisonment of up to 10 years if companies do not respect personal information and handle it with the utmost care and responsibility.[76] Data subjects whose personal information has been breached have recourse to civil remedies in terms of section 99 of the Act.[77]

As stated earlier, identity theft occurs when a person's personal information such as an identity document is wrongfully obtained and thereafter used to commit theft or fraud.[78] It is submitted that as POPI protects personal information, it will assist in addressing identity theft crimes. It will end the abusive and negligent use of personal information and unscrupulous information practices by companies by requiring companies to implement appropriate reasonable measures to prevent the unauthorised use of personal information.[79] Companies will have to invest in new technologies (such as encryption and access control) to prevent the unauthorised use of personal information. POPI also seeks to balance the right of privacy against economic and social progress. It will be interesting to see how POPI is interpreted by the courts in future cases.

4.1.2 The Electronic Communications and Transactions Act 25 of 2002 ("ECT")

The main aim of the ECT is to "provide for the facilitation and regulation of electronic communications and transactions in the public interest". The object of the ECT is set out in chapter 2, which recognises *inter alia* the importance of electronic communications and transactions to benefit South Africa and the need to develop a safe and secure environment for the consumer, business and the government to use electronic communications.[80] It should be noted that the term "data" refers to

---

75 See s 55 in ch 5 of POPI regarding the duties and functions of such officers.

76 See ss 107, 108 and 109 of POPI.

77 The Information Protection Regulator may pursue civil actions for damages for a breach of POPI's provisions, and a court hearing the matter, may award a just and equitable amount including the payment of damages as compensation for patrimonial and non-patrimonial loss suffered by the data subject.

78 See the discussion in ss 1 and 2 above.

79 See s 19 of POPI.

80 The term "consumer" refers to any natural person who enters or intends to enter into an electronic transaction with a supplier to receive the goods or services offered by the supplier. See ch 1 regarding definition of key terms. The object of the ECT is to protect the public (consumers, business and the government) who use electronic communications.

electronic representations of information in any form, whilst the term "electronic communication" refers to a communication by means of data messages.[81] According to section 85 of the ECT, the term "access" includes the action of a person who after considering any data becomes aware of the fact that he or she is not authorised to access that data, but nevertheless continues to access that data.[82] The computer may become the "subject" of a crime when it is used as an instrument to commit traditional crimes such as theft, fraud or new types of criminal activity such as identity theft.[83] Thus, identity theft can be regarded as an example of a cybercrime.

Cybercrime is addressed in Chapter 13 of the ECT, which contains the following: Anti-cracking (or anti-thwarting) and hacking law, which prohibits the selling, designing or the production of security circumventing technology has been introduced in sections 86(4) and 86(3);[84] e-mail bombing and spamming are regulated in sections 86(5) and 45 respectively;[85] and computer-related extortion, fraud and forgery are addressed in section 87.[86] It is a criminal offence to intentionally access or intercept any data without authority or permission in terms of section 86(1) of the ECT.[87] The criminal provisions are contained in section 89.[88] Section 89 prescribes a fine or imprisonment not exceeding five years. It is submitted that more stringent penalties are required to

---

81 It should be noted that the term "data message" refers to data that is generated, sent or received or stored by electronic means and includes voice used in an automated transaction and a stored record.

82 Section 85 is said to define cybercrime. See Snail 2009 http://goo.gl/QAscPb.

83 Cassim 2009 *PER* 36-37; Goodman and Brenner 2002 *IJLIT* 144-145.

84 A person may be guilty of an offence in terms of s 86(4) if he or she designs a programme to overcome copyright protection. See Snail 2009 http://goo.gl/QAscPb.

85 S 86(5) of the ECT addresses denial of service ("DOS") attacks, which may cause a computer system to be inaccessible to legitimate users. Spamming is regulated in s 45, which prevents unsolicited commercial communications. Also see Snail 2009 http://goo.gl/QAscPb.

86 S 87 of the ECT prohibits actions described in s 86 for the purpose of achieving any unlawful proprietary or pecuniary advantage by trying to blackmail another person or by making a false misrepresentation to obtain a monetary benefit. Forgery refers to the unlawful and intentional making of a false document to the actual or potential prejudice of another person. See Smith 2014 http://goo.gl/SvDuXn.

87 This means that a person who after accessing data (the electronic representation of information in any form) becomes aware that he or she does not have any legal authority or permission to access that data, nevertheless continues to access that data, then that person is guilty of an offence in terms of s 86 the ECT. Also see s 85 of the ECT regarding the definition of "access".

88 They have been criticised as not being stringent enough. The *Regulation of Interception of Communications and Provision of Communications-Related Information Act* 70 of 2002 ("RICA") is said to prescribe much harsher measures than the ECT. See van der Merwe *et al Information and Communications Technology Law* 75-78.

deter crafty and sophisticated cyber criminals such as online identity thieves, who may use the personal information of individuals without permission or authority to commit identity fraud or theft.

In instances where the offender uses a skimming device[89] to breach certain security measures, and he or she uses the data enclosed within the magnetic strip of a debit or credit card illegally or unlawfully, then the offender has contravened sections 86 or 87 of the ECT. Similarly, offenders may infringe the common law offence of fraud because they are guilty of committing fraudulent transactions by using the cloned debit or credit card. It is noteworthy that the ECT does not address the crime of identity theft *per se.* However, as identity theft may involve Internet fraud, it may conceivably fall within the ambit of sections 86 and 87 of the ECT.

The following section will examine legislation that has been introduced in the United States, the United Kingdom and India to address identity theft incidents or crimes. To this end, the promulgation of identity theft legislation and the protection of personal information legislation in these jurisdictions will be examined. The above jurisdictions were chosen for the comparative study because they have valuable experience addressing identity theft crimes and protecting personal information, and they have made concerted efforts to address identity theft crimes (as the following discussion will demonstrate). The aim of the comparative study is to ascertain whether South Africa can learn from the experiences or approaches in these jurisdictions.

4.2 International law

4.2.1 United States of America

The increasing use of foreign call centres such as Indian call centres by American companies has resulted in an increase in identity theft incidents in the United States.[90]

---

89 A skimming device refers to a special storage device that is used to steal a credit or debit card number when a person's card is being processed for payment at a retail store. The information encoded on the cards may be valuable to identity thieves, who may use the information to make telephonic or electronic purchases. See Ardé *Saturday Star Personal Finance* 3; DTI 2014 http://www.thedti.gov.za.

90 Grant 2006 *J Tech L & Pol'y* 1-21. This article examines the application of laws to transnational identity theft crimes.

This practice, whereby foreign companies are hired to perform a business transaction, is called "outsourcing".[91] This enterprise has led to Indian outsourcing firms having increased access to the private financial information of American citizens.[92] This raises the question of whether American consumers whose personal information is subject to this transnational data flow are adequately protected.

There has also been a surge in tax identity theft[93] in the United States. Tax identity theft is usually discovered when there is a dispute regarding the income that is reported to the Income Revenue Service ("IRS") and a filing of multiple returns arises.[94] Victims of tax identity theft are encouraged to report the theft to law enforcement agencies or to file a report with the Federal Trade Commission ("FTC") in the United States, which monitors identity theft nationwide.[95] The IRS has also established a special unit called the IRS Identity Protection Specialised Unit which assists taxpayers with tax identity issues.[96] Taxpayers are encouraged to avoid becoming victims by becoming aware of IRS practices and safeguarding their personal information on laptops, computers, smartphones and similar devices.[97] Thus a need arises for appropriate measures to be taken to effectively and speedily control this type of fraud.

4.2.1.1 Identity theft laws

Identity theft has become one of the fastest growing crimes in the United States, and it has been described as the top consumer complaint since the year 2000.[98] The *Identity Theft and Assumption Deterrence Act* ("ITAD") was enacted in 1998 in response to the growing problem of identity theft. It addressed network crimes. The

---

91 The rationale for this practice is usually cost savings to the American company. Grant 2006 *J Tech L & Pol'y* 4.

92 Grant 2006 *J Tech L & Pol'y* 5.

93 Taxpayers have had their identities stolen with the result that tax refunds are erroneously paid to fraudsters who have used the taxpayer's name. See Burquest and Wilkinson 2013 *Tax Adviser* 223. Also see Kari 2013 *Tax Adviser* 708.

94 See Burquest and Wilkinson 2013 *Tax Adviser* 223.

95 See Burquest and Wilkinson 2013 *Tax Adviser* 223.

96 Individuals whose accounts are subject to identity theft have also been given identity protection personal identification numbers (IP PINS). Burquest and Wilkinson 2013 *Tax Adviser* 224.

97 Burquest and Wilkinson 2013 *Tax Adviser* 223.

98 Lane and Sui 2010 *GeoJournal* 43. See Ravin 2008 *NJ Law* 60; Pierson 2007 *CILW* 22; Lynch 2005 *Berkeley Tech LJ* 261; Perl 2003 *J Crim L & Criminology* 172.

Act amended Title 18, US Code, section 1028 to make it a federal crime to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law".[99] The enactment of the *Identity Theft Act* made it possible to prosecute the fraudulent use of personal information, whether or not the information was contained in a physical document.[100] The *Identity Theft Act* also established the FTC as the lead agency to monitor, track and analyse complaints, and to disseminate information to consumers, researchers and law enforcement agencies.[101] The FTC has been logging increasing identity theft complaints and publishing the figures in annual reports since 2001.[102]

The *Identity Theft Penalty Enhancement Act*, 2004 was signed into law by President Bush on July 15, 2004. It was aimed at subjecting identity thieves to tougher penalties. The Act established a new crime, namely that of aggravated identity theft; that is, using a stolen identity to commit other crimes.[103] The *Identity Theft Enforcement and Restitution Act* of 2008 was signed into law by President Bush in 2008. Its aim was to enhance the identity theft laws. This Act applies to online and offline information theft, addresses phishing and identity theft, and authorises restitution to identity theft victims for the time they spend recovering from harm caused by identity theft.[104]

The *Fair and Accurate Credit Transactions Act* of 2003 ("FACT Act") was enacted *inter alia* to further address the problem of identity theft and further regulate the use of credit information. The FACT Act also imposes new business practices on companies that handle personal consumer information by requiring them to share with consumers

---

99 FBI 2014 http://goo.gl/TWBoep. Also see Lane and Sui 2010 *GeoJournal* 44; Winmill, Metcalf and Band 2010 *DE & ESLR* 25-26.

100 See Keenan 2005-2006 *Shidler J L Com & Tech* 5; Perl 2003 *J Crim L & Criminology* 172.

101 Lane and Sui 2010 *GeoJournal* 44. Also see Ravin 2008 *NJ Law* 63.

102 According to the FTC, an increase in technology-driven offences via the Internet and the illegal data mining of digital consumer databases will result in an increase in identity theft cases. See Lane and Sui 2010 *GeoJournal* 46.

103 This Act includes an additional two-year term of imprisonment for identity theft in connection with particular federal violations. See Winmill, Metcalf and Band 2010 *DE & ESLR* 25. Also see Sullins 2006 *Emory Int'l L Rev* 413-414 for a discussion about this Act.

104 Feigelson and Calman 2010 *J Internet L* 17. Also see Kim, Newberger and Shack 2012 *Am Crim L Rev* 476-477 for a discussion about identity theft legislation and penalties.

the collection, reporting and use of such consumer data.[105] The FACT Act is aimed at reducing consumers' vulnerability to identity theft and consumer fraud and minimising the harm once the theft or fraud has occurred. The FACT Act places responsibilities on businesses to co-operate fully with consumers through enhanced communication and more accurate recordkeeping.[106] The FACT Act has been commended for the increased power it provides to consumers regarding credit reporting and it calls for co-operation between the credit bureaus and the FTC to define and communicate to consumers a statement of their rights in the event that a theft or fraud occurs.[107] However, the FACT Act has also been criticised for not preventing the occurrence of identity theft in the first place, for not imposing sufficient restrictions and sufficient penalties on businesses and companies that violate the law, and for doing little to combat identity theft and fraud.[108] It has been reported that the judiciary has generally rejected victims' tort claims against businesses that are accused of creating opportunities for identity thieves, with the state of Alabama being an exception.[109] In *Patrick v Union State Bank*[110] it was held that a bank owes a duty of reasonable care to the person in whose name and upon whose identification an account is opened, to ensure that the person opening the account and to whom cheques are given is not an imposter. However, other courts have held that consumer protection matters should be addressed by legislators rather than judges, such as in *Huggins v Citibank NA*,[111] where it was held that the legislative branch is better equipped to assess and address the impact of fraud on victims and financial institutions.

Section 676 of the *Identity Theft and Tax Fraud Prevention Act* of 2013 also seeks to combat identity theft. A number of states have introduced identity theft laws with

---

105 See Keenan 2005-2006 *Shidler J L Com & Tech* 1 and Lynch 2005 *Berkeley Tech LJ* 278-281, for a discussion about this Act.

106 Keenan 2005-2006 *Shidler J L Com & Tech* 5; Newman *Identity Theft* 33.

107 Keenan 2005-2006 *Shidler J L Com & Tech* 6.

108 Keenan 2005-2006 *Shidler J L Com & Tech* 7-11.

109 The courts of Alabama recognised a claim of "negligent enablement of an imposter" while such a tort claim was rejected in other courts. Keenan 2005-2006 *Shidler J L Com & Tech* 9.

110 *Patrick v Union State Bank* 681 So2d 1364 (Ala 1996).

111 *Huggins v Citibank NA* 355 SC 329 (2003); 334. This court declined to recognise the tort of the negligent enablement of imposter fraud.

Arizona the first state to do so in 1996.[112] However, the types of laws that have been introduced differ according to the types of identity theft, the different punishments imposed, and the level of assistance that is rendered to victims. Some states such as California offer consumers an option to place an "anti-identity theft freeze" or "security freeze" on their credit record that will prevent organisations from examining their credit history and offering credit based on their record.[113] The security freeze provides greater protection by preventing any creditor from accessing any part of a consumer's credit history; however, it may create procedural difficulties and costs for those consumers who require the lifting of the freeze.[114] Identity theft insurance is also offered to some consumers.[115] However, these services have been criticised for benefiting the banks rather than consumers, and for their inability to alert the consumer or protect the consumer from criminal identity theft.[116]

The case of *United States v Rose*[117] illustrates the problem of synthetic identity theft. Synthetic identity theft occurs when the offender uses the victim's Social Security Number ("SSN") with a fake name, thus creating a new "synthetic" identity, or an offender can create a new identity using fabricated information, and this can be used to apply for credit.[118] The *Rose* case illustrates that individuals who become victims of synthetic identity theft may not suffer direct financial loss; however, they may suffer non-monetary loss such as reputational harm, emotional distress, and wastage of time and resources as a result of the debtor attempting to recover funds associated with the synthetic identity's account.[119]

---

112 See Perl 2003 *J Crim L & Criminology* 183-198 for a detailed discussion about these state laws. Also see Solove 2003 *Hastings Law Journal* 19-20.

113 See Lynch 2005 *Berkeley Tech LJ* 281-282 for a discussion about this type of protection. Also see Katel 2005 *CQ Researcher* 523.

114 Lynch 2005 *Berkeley Tech LJ* 282.

115 Regarding various types of insurance, see Lynch 2005 *Berkeley Tech LJ* 282-284.

116 Lynch 2005 *Berkeley Tech LJ* 284.

117 *United States v Rose* CR06-0787PHX (D Ariz Aug 22, 2006). In this case two men were charged with a variety of federal crimes for allegedly combining fabricated names with real Social Security Numbers from credit reports in order to apply for credit cards. Hoofnagle 2007 *Harv J L & Tech* 102.

118 Hoofnagle 2007 *Harv J L & Tech* 101.

119 Hoofnagle 2007 *Harv J L & Tech* 103.

4.2.1.2 Personal information laws

The United States of America does not have comprehensive data protection laws. Federal laws such as the *Right to Financial Privacy Act* of 1978 ("RFPA") and the *Electronic Communications Privacy Act* of 1986 ("ECPA") were introduced to prevent the government from violating people's privacy. However, these laws are not helpful for prosecuting identity thieves. The RFPA cannot be used against those individuals who steal outsourced information because the thieves are not American citizens, whilst the ECPA does not allow thieves to be prosecuted if they had authorisation to view the information, as have overseas outsourced employees.[120]

However, the *Computer Fraud and Abuse Act* of 1984 ("CFAA") provides a better foundation for identity theft claims such as those originating overseas. The CFAA provides civil remedies for certain types of computer crimes, and covers computers used by the federal government, financial institutions, or computers located outside the United States.[121] It is commendable that the CFAA does not permit the improper use of information when the thief at one point had authorisation to view the information.[122] The *Gramm-Leach-Bliley Privacy and Safeguards Rule* ("GLB Act") regulates information held by US financial institutions but it does not address trans-border flows directly.[123]

California state law currently protects people whose personal information has been stolen over the Internet. There are many laws which protect the personal information of consumers and hold businesses accountable for security breaches, such as the *California Online Privacy Protection Act*, the *California Security Act* and the *California Database Protection Act* ("CDPA").[124] The Choice Point incident was an example of the disclosure of information, in breach of security, to affected Californian clients and

120 Grant 2006 *J Tech L & Pol'y* 7.

121 18 USC s 1030. It is noteworthy that the CFAA regulates the monetary loss to be suffered to create a cause of action, and the use of compensatory damages and injunctive or other equitable relief for victims.

122 Grant 2006 *J Tech L & Pol'y* 7-8.

123 15 USC ss 6801-6827 (2000); Grant 2006 *J Tech L & Pol'y* 8. Also see Lynch 2005 *Berkeley Tech LJ* 265 for a discussion of this Act.

124 See Grant 2006 *J Tech L & Pol'y* 8-11 for a detailed discussion of these laws.

clients in other states.[125] The CDPA has been punted as a step in the right direction as it requires the disclosure of data breaches and allows for private causes of action.[126] It is also noteworthy that some American courts have found that the illegal use of personal information is foreseeable, and have imposed duties on businesses to protect personal information from illegal activity.[127]

It should be emphasised that the United States has not adopted uniform data protection standards equivalent to the *European Union Data Protection Directives* of 1995 ("EUDPD"). The EUDPD addresses the protection of individuals regarding the processing of personal data and it regulates the free movement of such data. It prevents European businesses from transacting with US companies in terms of article 1, which provides for the economic and social progress of the European Union (EU).[128] However, the United States Department of Commerce Safe Harbour Privacy Principles of 2000 (Safe Harbour Agreement) allows US businesses to self-certify that they are compliant with the standards of data protection adopted by EU nations through the EUDPD. This could be problematic.[129]

4.2.1.3 The role of the Federal Bureau of Investigation

The FBI has dedicated resources to combating and investigating identity theft. To illustrate this, it has combined forces with federal law enforcement agencies to arrest the following individuals during February 2013: some South Florida residents were charged in a $34 million stolen identity tax refund scheme involving the use of personal identification information by fraudsters to file false income tax returns with the Internal Revenue Service so that they could receive tax refund cheques, and in another instance, 18 people were charged in an international $200 million credit card fraud

---

125 ChoicePoint is a data brokering firm that announced that it had divulged the files of over 145 000 customers to thieves posing as legitimate small businesses. Grant 2006 *J Tech L & Pol'y* 9.

126 Grant 2006 *J Tech L & Pol'y* 21.

127 See *Remsberg v Docusearch* 149 NH 148, 816 A2d 1001 (2002) and *Bell v Michigan Council* 2005 WL 356306 (Mich Court of Appeal) respectively. Also see Bishop 2006-2007 *Shidler J L Com & Tech* 6-7.

128 Luck 2014 *De Rebus* 44-45.

129 There is a lack of practical control or enforcement that EU citizens can exert over American companies who have received their personal information. Very few American companies also comply with EUDPD principles. Luck 2014 *De Rebus* 45.

scam in which 7000 fake identities were invented to obtain thousands of fraudulent credit cards.[130] The role of the FBI in addressing identity theft crimes is commendable.

4.2.2 The United Kingdom

Banks in Britain are also facing e-commerce threats. Identity crimes have become one of the fastest growing types of fraud in the United Kingdom.[131] The UK's Fraud Prevention Service ("CIFAS") provides the UK's most comprehensive database of confirmed fraud data and an extensive range of fraud prevention services using the latest technology to protect organisations from the effects of fraud.[132] It comprises about 300 organisations from public and private sectors, such as banks, credit card bureaus, asset finance sectors, telecommunications and online retail sectors which share fraud information via the CIFAS. The aim is to prevent further fraud. British consumers are encouraged to contact the CIFAS to apply for protective registration. A new cyber reserve unit or force has also been created to strengthen national security by protecting computer networks and sensitive data, and to launch attacks and counter strikes against fraudsters.[133] The Ministry of Defence will also recruit reservist computer experts to work with regular armed forces to counter attacks in cyberspace.[134] An organisation called Action Fraud also investigates Internet crime in the UK, and consumers are urged to report phishing attacks and identity fraud to this organisation.[135] A National Cyber Crime Unit was also introduced in 2013 within the National Crime Agency to tackle cybercrime in the UK. Thus, UK consumers are receiving advice on protecting themselves from identity fraud through organisations such as the CIFAS and Action Fraud. The United Kingdom's National Hi-Tech Crime

---

130 FBI 2014 http://goo.gl/TWBoep. The FBI has also collaborated with the Justice Department, Secret Service and Postal Service and local, state and international law enforcement agencies to arrest and prosecute identity thieves. Lynch 2005 *Berkeley Tech LJ* 265.

131 CIFAS 2014 http://www.cifas.org.uk.

132 CIFAS 2014 http://www.cifas.org.uk.

133 Anon 2013 http://www.elaw@legalbrief.co.za.

134 Convicted computer hackers may also be recruited to help address the scourge of cybercrime.

135 Anon 2014 http://www.actionfraud.police.uk/fraud-az-phishing. For further information regarding the organisation, see Action Fraud 2014 http://www.actionfraud.police.uk accessed. It should be noted that phishing is considered to be a form of online identity theft. See the discussion in s 2 above.

Unit is working with the FBI to investigate phishing attacks in the UK.[136] This illustrates the importance of alliances to fight identity theft and phishing crimes.

The use of phishing scams to extract confidential account details from customers has proved costly to British banks according to recent reports.[137] However, the banks are stepping up their efforts to help consumers protect themselves from online scams and threats with the launch of a new website banksafeonline.org.uk.[138] Typically phishing attacks and identity scams have encompassed scam emails posing as security check emails from well-known banks, which attempt to trick users to hand over their account details and passwords. The details are then used to create fraudulent transfers. Most of the fraudulent activity is said to originate from Eastern Europe.[139] The aim of this site is to provide a one-stop advice shop for consumers and small businesses. It should be noted that UK banks rather than their customers bear the loss encountered as a result of phishing attacks and identity scams. It has been mooted that banks should educate their customers about the risks of transacting online and banks should employ more advanced data protection technology.[140] There have been some successful prosecutions: an American fugitive, Douglas Havard, was sentenced in 2005 to six years in a British prison for his part in a multi-million dollar international phishing scheme.[141] In a recent incident, a British couple faced a huge demand from German tax authorities for unpaid vat when the husband's passport was stolen.[142] The matter was eventually resolved.

136 For further information on the co-operation between law enforcement agencies, see Sullins 2006 *Emory Int'l L Rev* 411-412; Almahroos 2007-2008 *J L & Pol'y* 601.

137 Leyden 2004 http://goo.gl/lRouHP.

138 The site updates previous safe computing tips from banks and police regularly.

139 Leyden 2004 http://goo.gl/lRouHP.

140 See Leyden 2004 http://goo.gl/lRouHP.

141 Calman 2006-2007 *Rich J L & Tech* 10.

142 Mr Richard's passport was stolen in 2003 and his identity was used to conduct business operations in Germany. The German tax authorities have recently confirmed that they are no longer pursuing the unpaid VAT from Mr Richard. Winch 2013 http://goo.gl/vGR0vw; Winch 2013 http://goo.gl/DucEgQ.

4.2.2.1 Identity theft laws

The identity theft laws in the UK comprise the *Theft Act* of 1968, the *Data Protection Act* of 1998, the *Identity Cards Act* of 2006 and the *Fraud Act* of 2006.[143] The *Theft Act* of 1968 addresses theft, robbery and burglary. Stealing another person's identity is regarded as stealing a "property". An offender can be convicted of identity theft under this law; hence the *Theft Act* is relevant to prosecute identity thieves. According to the *Data Protection Act* of 1998, private information such as a person's ethnic identity, sexual orientation, religious affiliation, financial records, birth records and family records cannot be divulged. It is a privacy act that requires public entities to closely guard identity information. Agencies that hold mass data on the UK population cannot disclose such data to other entities without explicit consent, and it limits the period of time that a data reservoir can hold information. UK citizens have a right to obtain collected information about them, and organisations that store personal information must ensure that data protection systems are up to date and fully functioning.

The *Identity Cards Act* of 2006 enables the institution of the National Identity Register which issues identification cards and passports; enables background checks to verify the accuracy of collected data and to confirm citizens' identities. The law seeks to protect against personal identity theft and fraud; it legitimises the collection of personal information without consent for crime and justice purposes and it addresses identity theft crimes and identity fraud relating to identity cards.

The *Fraud Act* of 2006 targets phishing and pharming; prevents the misrepresentation of one's identity and the assumption of the identity of someone else, and outlaws the sending of emails that enable hackers to use and abuse personal and business information. It has introduced a new offence of "fraud": which can be committed by false representation, failure to disclose information and the abuse of one's position.[144] This Act requires the prosecution to prove that the offender knew that the article was

143 For further information regarding these laws, see Experian 2014 http://www.experian.co.uk and the website, National Archives 2014 http://www.legislation.gov.uk.

144 Savirimuthu 2008 *JICLT* 121-122. It is noteworthy that computer-related fraud is addressed in A 8 of the *Convention on Cybercrime* (2001).

designed or adapted for use in the course of or in connection with fraud, and intended it to be used to commit, or assist in the commission of fraud.[145] The *Fraud Act* is seen as a step in the right direction as it removes deficiencies in the previous regime on fraud and it incorporates principles which conform to the concept of technological neutrality.[146]

European Union laws such as the *European Union Data Protection Directives* of 1995 ("EUDPD") have created uniform standards of data privacy for all member states (such as the UK), with the result that businesses within the EU that are reliant on data can easily transact with one another.[147] This has assisted economic and social progress among signatories of the EUDPD, but it presents challenges when EU member states conduct business in jurisdictions that have lesser data privacy regulations than their own, such as the United States.

4.2.3 India

Identity theft has become one of the growing concerns in cybercrime in India today. India is fast emerging as a soft target for organised cybercrime, with many Indians becoming victims of identity theft. Identity theft cases are increasing in India with cybercrime enforcement agencies in Indian cities investigating such crimes.[148] Instances of identity theft are increasing as more Indians log onto the Internet. A survey by Microsoft has found that damages from online identity theft have cost Indians Rs7,500 on average.[149] Identity theft therefore has serious financial implications.

---

145 Savirimuthu 2008 *JICLT* 122.

146 Savirimuthu 2008 *JICLT* 122.

147 A 25 of the *European Union Data Protection Directives* (1995) prohibits transborder information flows to countries with lesser data privacy protection than member states. Luck 2014 *De Rebus* 44.

148 See Dhankhar 2014 http://goo.gl/iaC2wf; Vidyalaxmi 2012 http://goo.gl/Hh2uTf.

149 Microsoft Corporation 2014 http://www.Downloads/2013_MCSI_Worldwide_Results_Executive_Summary.pdf; Anon 2014 http://goo.gl/WTQUvg.

4.2.3.1 Identity theft laws

Previously, identity theft was not addressed separately in Indian law, but it fell within the ambit of "hacking", which involved the infiltration of a computer resource involving the "alteration, deletion or destruction of the information residing therein, facilitating the crime of identity theft".[150] The *Information Technology Act* of 2000 ("ITA") and the Indian Penal Codes imposed criminal sanctions on thieves who used computers to commit crimes.[151] The enforcement of these laws presented many challenges. The ITA did not contain a specific provision to address identity theft. However, it established the Cyber Regulations Appellate Tribunal to adjudicate cybercrimes such as identity theft. During February 2003 a Delhi High Court sentenced a call centre employee for online cheating.[152] The ITA was subject to criticism due to its lack of enforcement and few successful prosecutions.[153] Thus, a need arose for a more comprehensive response to identity theft by Indian legislators.

The object of the *Information Technology Amendment Act* of 2008 (ITAA) was to protect e-commerce and e-transactions involving information exchange and electronic data exchange.[154] It introduced new offences in sections 66A to 66F. They specifically address the offence of identity theft and identity fraud by use of the Internet.[155] Section 66C addresses punishment for identity theft and section 66D addresses punishment for cheating by impersonation by using a computer resource. Therefore, identity theft is now a punishable offence and the theft of any feature associated with the identity of a person includes impersonation by making use of electronic signature, password or any other unique identification feature. The penalties comprised a term of imprisonment which may extend to three years and a fine which may extend to

150 Moharty 2011 *IJLT* 112.
151 For a detailed discussion of these laws, see Grant 2006 *J Tech L & Pol'y* 11-14. Also see Sandeepan "Identity Theft" 115 for a discussion of the ITA.
152 The accused had stolen an American citizen's credit card information to purchase a colour television and a telephone. Grant 2006 *J Tech L & Pol'y* 14.
153 Grant 2006 *J Tech L & Pol'y* 14.
154 Moharty 2011 *IJLT* 111.
155 See ss 66C and 66D in the ITAA.

rupees of one lakh.[156] Therefore, any person found guilty in terms of the ITAA will be subject to imprisonment and a stiff monetary fine. The ITAA has been subject to criticism as a result of its poor drafting, and the lack of a comprehensive provision addressing punishment.[157] A computer emergency response team (Cert-In) has been established in India to operate as a central access point for the troubleshooting, reporting and detection of crimes related to identity theft and other computer security issues.[158]

India does not have many laws that explicitly prescribe or prohibit systematic government access to private sector data.[159] The *Information Technology Amendment Act* of 2008 allows authorised agencies broad reactive access to personal information held by the private sector for investigation purposes.[160] However, the Indian government's access to and disclosure of private sector data has been criticised because it does not adopt principles of natural justice and its practices are susceptible to corruption and collusion.[161]

The above discussion demonstrates that the United States, the United Kingdom, India and South Africa are making concerted efforts to tackle identity theft crimes. Legislation in the United States, such as the *Identity Theft Enforcement and Restitution Act* of 2008, the *Identity Theft and Tax Fraud Prevention Act* of 2013 and the FACT Act demonstrate the government's commitment to combat identity theft. The roles of the FTC and the FBI in investigating and tracking down identity theft cases are also commendable. However, the United States needs to adopt uniform data protection standards similar to the EUDPD Directives in Europe. Similarly, the promulgation of the *Fraud Act* of 2006 in the UK, and the role of organisations such as Action Fraud and CIFAS demonstrate the UK's commitment to tackling the scourge of identity theft. The importance of alliances to fight identity theft crimes as

---

156 See s 66C. This section has been criticised by Moharty as the means by which the identifying information is accessed is discounted but only the act of making fraudulent or dishonest use of the information itself is criminalised. Moharty 2011 *IJLT* 112.

157 Moharty 2011 *IJLT* 113, 119.

158 See DeitY 2014 http://www.deity.gov.in/content/icert.

159 See Abraham and Hickok 2012 *IDPL* 302.

160 However, they do not establish grounds for access for example, for reasons of national security. Abraham and Hickok 2012 *IDPL* 305.

161 Abraham and Hickok 2012 *IDPL* 315.

demonstrated by the co-operation between the United Kingdom's National Hi-Tech Crime Unit and the FBI is recognised. Legislation such as the ITAA in India, and POPI and the ECT in South Africa are seen as steps in the right direction in combating identity theft crimes in these countries. The introduction of a Cybersecurity Policy Framework in South Africa to respond to cyber security threats is lauded, but it needs to be implemented. However, all countries need to ensure that their fight against identity theft does not jeopardise basic human rights and fundamental freedoms such as the rights to privacy and access to information. To this end, a balance should be struck between access to information by institutions that have a legitimate use for such information, and respecting the rights of individuals and or consumers. Incentives should also be provided to businesses and institutions to exercise reasonable care to safeguard the personal information of individuals in this technological age.

5 Conclusion

Identity theft has become a serious and growing problem worldwide, and it occurs by conventional means and in cyberspace.[162] It cost the US economy about $24.7 billion during 2012; the cost to the British economy is reported to be £1.3 billion annually whilst it has cost the South African economy about R1 billion a year.[163] The use of new technologies has resulted in increased opportunities for criminals to steal and illegally use personal information to commit identity theft crimes.[164] It is submitted that identity theft is increasingly challenging law enforcement agencies and governments around the world. The time and money spent in responding to identity theft crimes can also be extensive.[165] Improved technology and consumer awareness have also been punted as additional measures to address the scourge of identity theft.[166] Consumers should be educated about the risks of transacting online, their

---

162 See Microsoft Corporation 2014 http://www.Downloads/2013_MCSI_Worldwide_Results_Executive_Summary.pdf.

163 Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html; Pierson 2007 *CILW* 22; Ardé *Saturday Star* 3.

164 Perl 2003 *J Crim L & Criminology* 174. Also see Nuth 2008 *CLSR* 437-438.

165 Pierson 2007 *CILW* 25.

166 Nuth 2008 *CLSR* 416, 429-432. Also see Ogwezzy 2012 *AIJJS* 97-100 for a discussion of strategies to address the menace of cybercrime. Also see Savirimuthu 2008 *JICLT* 126, regarding the need for technological solutions, the education of consumers and the active role of computer organisations. Also see Black 2005 *JLIS* 88-90; Almahroos 2007-2008 *J L & Pol'y* 603-604.

rights regarding online fraud and measures to prevent and respond to identity theft.[167] Technical solutions are seen as a positive response to address vulnerabilities in computer networks. Organisations and Internet service providers should also educate users regarding safe browsing and make safety packages available to their users.[168] It has been mooted that there should be mandatory public reporting of identity theft cases by financial institutions and that they should report regularly to a financial regulator.[169] It is proposed that such reporting will improve our understanding of identity theft and enable policymakers to enact adequate preventive measures to respond to the severity and methods of the crime.[170] It is submitted that technical solutions and/or education should form part of legislative interventions to address identity theft crimes.

Criminal law should be effectively utilised to ensure that procedural or technical obstacles do not obstruct the prosecution of the online fraudster.[171] Financial institutions should also publicly report on identity theft incidents without infringing on the rights of the consumer, and this will create a market for identity theft prevention. They should also offer safe products that will help consumers make informed choices. Businesses should not only adopt the business practices required under legislation such as the FACT Act and POPI, but should also focus on emerging practices that might further protect consumers against identity theft. There is also a need for legislation to be enacted to provide consumers and businesses with weapons to pre-empt the damage and prevent the occurrence of the identity theft. Businesses must also use more advanced technology to combat security weaknesses in our current technological environment. Our technology industry also has to ensure that our system of data protection is coherent and that it conforms to current technological practices. It is also important to remember that "computers do not steal identities… but people do".[172] Therefore, a better understanding of the offenders and transgressors will also

167 Lynch 2005 *Berkeley Tech LJ* 276.
168 Lynch 2005 *Berkeley Tech LJ* 276.
169 For information on the reporting process, see Hoofnagle 2007 *Harv J L & Tech* 108-112.
170 Hoofnagle 2007 *Harv J L & Tech* 122.
171 Savirimuthu 2008 *JICLT* 122.
172 As observed by Collins *Investigating Identity Theft* 181. Also see Lane and Sui 2010 *GeoJournal* 46.

aid in slowing the progress of identity theft. The importance of alliances between different government law enforcement agencies to combat identity theft across different jurisdictions is acknowledged, as demonstrated by the co-operation between the UK's Hi-Tech Crime Unit and the FBI.[173] The International Criminal Police Organisation also facilitates co-operation between law enforcement agencies to investigate online crimes.[174] Identity theft is a growing and evolving problem existing in the physical and virtual worlds, and it requires a multi-faceted and multi-disciplinary approach by law enforcement agencies, businesses, consumers and collaboration between countries.

It has been mooted that the following steps[175] should be taken to respond to identity theft:

- Raise businesses' awareness of their responsibility to protect employee and client records (such as the enactment of GLB/*Gramm-Leach-Bliley* Act and the FACT Act in the US, which require certain businesses or institutions to protect information better, and POPI in South Africa).
- Educate individuals and consumers about protecting their personal information (offline and online).
- Form alliances between different law enforcement agencies to combat identity theft in different jurisdictions (as illustrated by the co-operation between the UK's Hi-Tech Crime Unit and the FBI).
- Create collaboration between governments and other service organisations to protect personal information of private individuals and public bodies.
- Work with local banks to encourage credit card bureaus to adopt improved security practices for their clients and or customers.
- Track the delivery of documents to avert the theft of personal information.
- Work with identity theft victims to provide assistance and advice regarding their rights.

---

173 Sullins 2006 *Emory Int'l L Rev* 411-412; Almahroos 2007-2008 *J L & Pol'y* 601.

174 Sullins 2006 *Emory Int'l L Rev* 411-412.

175 See Newman *Identity Theft* 32-41 for a detailed discussion of these steps/responses. Also see Ravin 2008 *NJ Law* 63 regarding a checklist for representing identity theft victims, and Pierson 2007 *CILW* 22-24, regarding steps to reduce identity theft.

- Devise a plan to prevent or minimise the harm of identity theft when large identity databases have been breached.

It is submitted that these steps are commendable and should be followed to combat identity theft and assist the victims. Further steps to curtail identity theft should include a speedier and increased intervention by intermediary parties (such as financial institutions, law enforcement agencies and criminal record departments) between the victim and the identity thief, the use of an identity fraud alert registry, and the increased use of biometric data (such as finger prints, retina scans and hand imaging) to identify individuals.[176] Therefore, it is imperative that countries should amend their laws to better address identity theft and the problems associated with it. The challenge is to formulate policies that strike a balance allowing reasonable access to information by people who have a legitimate use for such information (the "collectors"), and at the same time to afford protection to individuals and/or consumers. Incentives should also be provided to businesses and institutions to exercise reasonable care to prevent the further abuse and negligent disclosure of the personal information of individuals and/or consumers.

176 Perl 2003 *J Crim L & Criminology* 198-207.

BIBLIOGRAPHY

Literature

Abraham and Hickok 2012 *IDPL*

Abraham S and Hickok E "Government Access to Private-Sector Data in India" 2012 *IDPL* 302-314

Almahroos 2007-2008 *J L & Pol'y*

Almahroos R "Phishing for the Answer: Recent Developments in Combating Phishing" 2007-2008 *J L & Pol'y* 595-621

Ardé *Saturday Star*

Ardé A "Identity Fraud on the Rise" *Saturday Star* (6 September 2014) 3

Ardé *Saturday Star Personal Finance*

Ardé A "Banks Must Up Their Game, or Cough Up" *Saturday Star Personal Finance* (29 November 2014) 3

Bishop 2006-2007 *Shidler J L Com & Tech*

Bishop DA "To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?" 2006-2007 *Shidler J L Com & Tech* 3-9

Black 2005 *JLIS*

Black P "Phish to Fry: Responding to the Phishing Problem" 2005 *JLIS* 73-91

Burquest and Wilkinson 2013 *Tax Adviser*

Burquest P and Wilkinson J "Is Tax Identity Theft Becoming an Epidemic?" April 2013 *Tax Adviser* 223-224

Calman 2006-2007 *Rich J L & Tech*

Calman C "Bigger Phish to Fry: California's Anti-Phishing Statute and Its Potential Imposition of Secondary Liability on Internet Service Providers" 2006-2007 *Rich J L & Tech* 1-24

Cassim 2009 *PER*

Cassim F "Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study" 2009 *PER* 36-79

Cassim 2012 *PER*

Cassim F "Addressing the Spectre of Cyber Terrorism: A Comparative Perspective" 2012 *PER* 381-415

Cherry 2005-2006 *J L & Pol'y*

Cherry SA "The Effect of Spyware and Phishing on the Privacy Rights of Internet Users" 2005-2006 *J L & Pol'y* 573-598

Collins *Investigating Identity Theft*

Collins JM *Investigating Identity Theft: A Guide for Businesses, Law Enforcement, and Victims* (Wiley Hoboken 2006)

Feigelson and Calman 2010 *J Internet L*

Feigelson J and Calman C "Liability for the Costs of Phishing and Information Theft" April 2010 *J Internet L* 1-26

Goodman and Brenner 2002 *IJLIT*

Goodman MD and Brenner S "The Emerging Consensus on Criminal Conduct in Cyberspace" 2002 *IJLIT* 139-222

Grant 2006 *J Tech L & Pol'y*

Grant S "'I Just Bought a Flat Screen TV in Kolkata?' Application of Laws for International Outsourcing Related Identity Theft" 2006 *J Tech L & Pol'y* 1-21

Harrell and Langton *Victims of Identity Theft*

Harrell E and Langton L *Victims of Identity Theft* (US Department of Justice Washington DC 2013)

Hoofnagle 2007 *Harv J L & Tech*

Hoofnagle CJ "Identity Theft: Making the Known Unknowns Known" 2007 *Harv J L & Tech* 98-122

Kari 2013 *Tax Adviser*

Kari ES "At Least You Still Have Your Identity" October 2013 *Tax Adviser* 708-709

Katel 2005 *CQ Researcher*

Katel P "Identity Theft: Can Congress Give Americans Better Protection" June 2005 *CQ Researcher* 517-540

Keenan 2005-2006 *Shidler J L Com & Tech*

Keenan TJ "The Fact Act of 2003: Securing Personal Information in an Age of Identity Theft" 2005-2006 *Shidler J L Com & Tech* 1-16

Kim, Newberger and Shack 2012 *Am Crim L Rev*

Kim C, Newberger B and Shack B "Computer Crimes" 2012 *Am Crim L Rev* 444-486

Lane and Sui 2010 *GeoJournal*

Lane GW and Sui DZ "Geographies of Identity Theft in the US: Understanding Spatial and Demographic Patterns, 2002-2006" 2010 *GeoJournal* 43-55

Luck 2014 *De Rebus*

Luck R "POPI - Is South Africa Keeping up with International Trends?" May 2014 *De Rebus* 44-46

Lynch 2005 *Berkeley Tech LJ*

Lynch J "Identity Theft in Cyber Space: Crime Control Methods and Their Effectiveness in Combating phishing Attacks" 2005 *Berkeley Tech LJ* 259-300

Moharty 2011 *IJLT*

Moharty A "New Crimes under the Information Technology (Amendment) Act" 2011 *IJLT* 103-120

Newman *Identity Theft*

Newman GR *Identity Theft* (US Deptartment of Justice, Office of Community Oriented Policing Services Washington DC 2004)

Nuth 2008 *CLSR*

Nuth MS "Taking Advantage of New Technologies: For and Against Crime" 2008 *CLSR* 437-446

Ogwezzy 2012 *AIJJS*

Ogwezzy MC "Cyber Crime and the Proliferation of Yahoo Addicts in Nigeria" 2012 *AIJJS* 86-102

Perl 2003 *J Crim L & Criminology*

Perl MW "It's Not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft" 2003 *J Crim L & Criminology* 169-208

Pierson 2007 *CILW*

Pierson CT "Understanding Identity Theft and Stopping the Crime" March 2007 *CILW* 22-26

Ravin 2008 *NJ Law*

Ravin RL "Avoiding Online Identity Theft and Representing Its Victims" December 2008 *NJ Law* 60-65

Rubin, Fraser and Smith 1995 *International Journal of Law and Information Technology*

Rubin H, Fraser L and Smith M "US and International law aspects of the Internet: Fitting square pegs into round holes" 1995 *International Journal of Law and Information Technology* 117-143

Sandeepan "Identity Theft"

Sandeepan N "Identity Theft in Cyberspace with Special Reference to India" *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)* (15-17 January 2011 Jaipur) 113-115

Savirimuthu 2008 *JICLT*

Savirimuthu J "Identity Theft and the Gullible Computer User: What Sun Tzu and the *Art of War* Might Teach" 2008 *JICLT* 120-128

Snyman *Criminal Law*

Snyman CR *Criminal Law* 6th ed (LexisNexis Durban 2014)

Solove 2003 *Hastings Law Journal*

Solove DJ "Identity Theft, Privacy, and the Architecture of Vulnerability" 2003 *Hastings Law Journal* 1-46

Stevenson 2005 *Duke Law and Technology Review*

Stevenson RLB "Plugging the 'phishing' hole: Legislation versus Technology" 2005 *Duke Law and Technology Review* 1-14

Sullins 2006 *Emory Int'l L Rev*

Sullins LL "'Phishing' for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft" 2006 *Emory Int'l L Rev* 397-433

Thakali *Saturday Star*

Thakali T "New Legislation Comes Too Late for Identity Theft Victims" *Saturday Star* (30 November 2013) 7

Van der Merwe *et al Information and Communications Technology Law*

Van der Merwe DP *et al Information and Communications Technology Law* (LexisNexis Durban 2008)

Winmill, Metcalf and Band 2010 *DE & ESLR*

Winmill BL, Metcalf DL and Band ME "Cybercrime: Issues and Challenges in the United States" 2010 *DE & ESLR* 19-34

Case law

United States of America

Bell v Michigan Council 2005 WL 356306 (Mich Court of Appeal)

Huggins v Citibank NA 355 SC 329 (2003)

Patrick v Union State Bank 681 So2d 1364 (Ala 1996)

Remsberg v Docusearch 149 NH 148, 816 A2d 1001 (2002)

Renor v ACLU US 844, 851 (1997)

United States v Rose CR06-0787PHX (D Ariz Aug 22, 2006)

Legislation

India

Information Technology Act of 2000

Information Technology Amendment Act of 2008

South Africa

Constitution of the Republic of South Africa, 1996

Criminal Law Amendment Act 105 of 1997

Electronic Communications and Transactions Act 25 of 2002

Protection of Personal Information Act 4 of 2013

Regulation of Interception of Communications and Provision of Communications Related Information Act 70 of 2002

United Kingdom

Data Protection Act of 1998

Fraud Act of 2006

Identity Cards Act of 2006

Theft Act of 1968

United States of America

California Database Protection Act of 2003

California Online Privacy Protection Act of 2003

California Security Act of 2003

Computer Fraud and Abuse Act of 1984

Electronic Communications Privacy Act of 1986

Fair and Accurate Credit Transactions Act of 2003

Gramm-Leach-Bliley Act of 1999

Identity Theft and Assumption Deterrence Act of 1998

Identity Theft Enforcement and Restitution Act of 2008

Identity Theft Penalty Enhancement Act of 2004

Identity Theft and Tax Fraud Prevention Act of 2013

Right to Financial Privacy Act of 1978

International instruments

Convention on Cybercrime (2001)

European Union Data Protection Directives (1995)

Internet sources

Action Fraud 2014 http://www.actionfraud.police.uk

Action Fraud 2014 *Home Page* http://www.actionfraud.police.uk accessed 21 August 2014

Anon 2013 http://www.fin24.com/Economy/Beware-new-identity-theft-scam-20130408

Anonymous 2013 *Beware new software Identity theft scam* http://www.fin24.com/Economy/Beware-new-identity-theft-scam-20130408 accessed 10 April 2013

Anon 2014 http://goo.gl/WTQUvg

Anonymous 2014 *Identity Theft Cases Costs Every Indian Netizen Rs 7,500: Microsoft* http://goo.gl/WTQUvg accessed 21 August 2014

Anon 2014 http://www.actionfraud.police.uk/fraud-az-phishing

Anonymous 2014 *Phishing* http://www.actionfraud.police.uk/fraud-az-phishing accessed 5 May 2014

CIFAS 2014 http://www.cifas.org.uk

CIFAS 2014 *Home Page* http://www.cifas.org.uk accessed 19 August 2014

DeitY 2014 http://www.deity.gov.in/content/icert

Department of Electronics and Information Technology, Government of India 2014 *India Computer Emergency Response Team (ICERT)* http://www.deity.gov.in/content/icert accessed 15 December 2014

Dhankhar 2014 http://goo.gl/iaC2wf

Dhankhar L 2014 *Identity Theft Cases on the Rise* http://goo.gl/iaC2wf accessed 21 August 2014

DTI 2014 http://www.thedti.gov.za

Department of Trade and Industry 2014 *Identity Theft Scams* http://www.thedti.gov.za accessed 2 September 2014

Experian 2014 http://www.experian.co.uk

Experian 2014 *Identity Theft* http://www.experian.co.uk accessed 19 August 2014

FBI 2014 http://goo.gl/TWBoep

Federal Bureau of Investigation 2015 *Identity Theft Overview* http://goo.gl/TWBoep accessed 6 May 2014

Gercke 2011 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html

Gercke M 2011 *Understanding Cybercrime: A Guide for Developing Countries* http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html accessed 14 July 2014

Jones 2014 http://goo.gl/MCVT4c

Jones G 2014 *South Africa Neglects Alarming Effect of Cybercrime* http://goo.gl/MCVT4c accessed 9 December 2014

Leyden 2004 http://goo.gl/lRouHP

Leyden J 2004 *UK Banks Launch Anti-phishing Website* http://goo.gl/lRouHP accessed 5 May 2014

Microsoft Corporation 2014

http://www. Downloads/2013_MCSI_Worldwide_Results_Executive_Summary. pdf. Microsoft Corporation 2014 *2013 Microsoft Computing Safety Index (MCSI) Worldwide Results Summary* http://www.Downloads/2013_MCSI_Worldwide_ Results_Executive_Summary.pdf accessed 19 November 2014

National Archives 2014 http://www.legislation.gov.uk

National Archives 2014 *UK Legislation Home Page* http://www.legislation.gov.uk accessed 9 December 2014

SABRIC 2014 https://www.sabric.co.za

South Africa Banking Risk Information Centre 2014 *Home Page* https://www.sabric.co.za accessed 8 July 2014

SAFPS 2014 http://www.safps.org.za

Southern African Fraud Prevention Service 2014 *Home Page* http://www.safps.org.za accessed 2 September 2014

SARS 2014 http://www.sars.gov.za/TargTax/Crime/Pages/Identity.Fraud.aspx

South African Revenue Service 2014 *Identity Fraud* http://www.sars.gov.za/TargTax/Crime/Pages/Identity.Fraud.aspx accessed 9 December 2014

Smith 2014 http://goo.gl/SvDuXn

Smith T 2014 *Identity Theft* http://goo.gl/SvDuXn accessed 2 September 2014

Snail 2009 http://goo.gl/QAscPb

Snail S 2009 *Cyber Crime in South Africa – Hacking, Cracking, and Other Unlawful Online Activities* http://goo.gl/QAscPb accessed 11 December 2014

Tamarkin 2014 http://goo.gl/pmLxZb

Tamarkin E 2014 *ISS: SA Must Pay More Attention to Cybercrime* http://goo.gl/pmLxZb accessed 25 November 2014

Vidyalaxmi 2012 http://goo.gl/Hh2uTf

Vidyalaxmi ET 2012 *Cybercrime: Beware of Identity Theft* http://goo.gl/Hh2uTf accessed 21 August 2014

Waugh 2014 http://www.welivesecurity.com/2014/02/12

Waugh R 2014 *Worldwide Costs of Identity Theft* http://www.welivesecurity.com/2014/02/12 accessed 9 December 2014

Winch 2013 http://goo.gl/vGR0vw

Winch J 2013 *Our £ 130,000 Bill from Identity Theft* http://goo.gl/vGR0vw accessed 19 August 2014

Winch 2013 http://goo.gl/DucEgQ

Winch J 2013 *German Taxman Backs Down in UK's Worst Case of Identity Theft* http://goo.gl/DucEgQ accessed 21 August 2014

LIST OF ABBREVIATIONS

AIJJS	AGORA International Journal of Juridical Sciences
Am Crim L Rev	American Criminal Law Review
APWG	Anti-Phishing Working Group
Berkeley Tech LJ	Berkeley Technology Law Journal
CDPA	California Database Protection Act (USA)
CERTs	Computer Emergency Readiness Teams
CFAA	Computer Fraud and Abuse Act (USA)
CIFAS	United Kingdom Fraud Prevention Service
CILW	Computer and Internet Lawyer
CSLR	Computer Law and Security Report
DE & ESLR	Digital Evidence and Electronic Signature Law Review
DeitY	Department of Electronics and Information Technology, Government of India
DOS	Denial of service
DTI	Department of Trade and Industry (RSA)
ECPA	Electronic Communications Privacy Act
ECT	Electronic Communications and Transactions Act (RSA)
Emory Int'l L Rev	Emory International Law Review
EU	European Union
EUDPD	European Union Data Protection Directives
FACT Act	Fair and Accurate Credit Transactions Act (USA)
FBI	Federal Bureau of Investigation (USA)
FTC	Federal Trade Commission (USA)
GLB Act	Gramm-Leach-Bliley Act (USA)

HANIS	Home Affairs National Identification System (RSA)
Harv J L & Tech	Harvard Journal of Law and Technology
IDPL	International Data Privacy Law
IJLIT	International Journal of Law and Information Technology
IJLT	Indian Journal of Law and Technology
IJTPL	International Journal of Technology Policy and Law
IP PINS	Identity protection personal identification numbers
IRS	Income Revenue Service (USA)
ITA	Information Technology Act (India)
ITAA	Information Technology Amendment Act (India)
ITAD	Identity Theft and Assumption Deterrence Act (USA)
J Crim L & Criminology	Journal of Criminal Law and Criminology
J Internet L	Journal of Internet Law
J L & Pol'y	Journal of Law and Policy
J Tech L & Pol'y	Journal of Technology Law and Policy
JICLT	Journal of International Commercial Law and Technology
JLIS	Journal of Law, Information and Science
MCSI	Microsoft Computing Safety Index
NJ Law	New Jersey Lawyer
PER	Potchefstroom Elektroniese Regstydskrif
POPI	Protection of Personal Information Act (RSA)
RICA	Regulation of Interception of Communications and Provision of Communications-Related Information Act (RSA)
Rich J L & Tech	Richmond Journal of Law and Technology
RFPA	Right to Financial Privacy Act (USA)
SABRIC	South Africa Banking Risk Information Centre
SAFPS	Southern African Fraud Prevention Service
SARS	South African Revenue Service

Shidler J L Com & Tech	Shidler Journal of Law, Commerce and Technology
SSN	Social security number

PROTECTING PERSONAL INFORMATION IN THE ERA OF IDENTITY THEFT: JUST HOW SAFE IS OUR PERSONAL INFORMATION FROM IDENTITY THIEVES?

F Cassim*

SUMMARY

Identity theft has become one of the fastest growing white collar crimes in the world. It occurs when an individual's personal information such as *inter alia* his or her name, date of birth or credit card details is used by another individual to commit identity fraud. Identity theft can be committed via physical means or online. The increased use of the Internet for business and financial transactions, social networking and the storage of personal information has facilitated the work of identity thieves. Identity theft has an impact on the personal finances and emotional well-being of victims, and on the financial institutions and economies of countries. It presents challenges for law enforcement agencies and governments worldwide. This article examines how identity thieves use the personal information of individuals to commit identity fraud and theft, and looks at legislative solutions introduced in South Africa, the United States of America, the United Kingdom and India to combat identity theft crimes. The article examines measures introduced by the respective governments in these countries to counteract such crimes. Finally, the article will propose a way forward to counteract such crimes in the future. The study reveals that identity theft is a growing and evolving problem that requires a multi-faceted and multi-disciplinary approach by law enforcement agencies, businesses, individuals and collaboration between countries. It is advocated that businesses and institutions should take measures to protect personal information better and that individuals should be educated about their rights, and be vigilant and protect their personal information offline and in cyberspace.

* Fawzia Cassim. BA (UDW) LLB (Univ Natal) LLM LLD (UNISA). Associate Professor, Department of Criminal and Procedural Law, UNISA and admitted attorney and conveyancer. Email: cassif@unisa.ac.za.

KEYWORDS: Identity theft; fraud; theft; cybercrime; personal information; data; Internet; cyberspace; right to privacy; computer users; law enforcement agencies; businesses; legislation; South Africa; United States of America; United Kingdom; India.