IDENTITY THEFT- A CRITICAL AND COMPARATIVE ANALYSIS OF VARIOUS LAWS IN INDIA

Aishwarya Joshi[1]

INTRODUCTION

The mechanization of the world and the storage of information in form of binary data, in storage devices such as computers have truly made it possible to keep track of various data in an efficient manner. With the invention of the World Wide Web by Tim Berners Lee, it is now possible for people to interact with several people and transact various businesses all at the same time through the internet. The earliest computer was the Electronic Numerical Integrator Analyzer and Computer (ENIAC), used to do ballistic calculations for the U.S. military during the World War II.[2] With the advent of microprocessor and subsequently the microcomputers (also called personal computers) , the idea of putting a computer to exclusive use of an individual came up as it became affordable and reduced in size.[3] The use of computers did away with manual storage and management of information and finding a particular piece of stored information became easier. The evolution of computer technology and increased human interactions using computers, has led to myriad offenses or illegal practices (called cybercrimes) in this arena as well. One such crime is identity theft.

Identity theft refers to all types of crimes wherein a person fraudulently obtains another person's personal information and uses it primarily for economic gain.[4] Identity theft can be understood as a sub set of data theft wherein personal information of an individual forms the data stolen and is the means to perpetrate several other crimes. It has emerged to be one of the fastest growing crimes in America and several other countries.[5] This is primarily because, in America, all the personal identification information has been linked to a single Social

[1] 3rd Year B.A-LLB (Honors) Student, NALSAR University of Law, Hyderabad.
[2] HISTORY.com, Invention of the PC - Inventions - HISTORY.com (2011), available at www.history.com/topics/inventions/invention-of-the-pc (last visited Oct 13, 2015).
[3] History of Computers, available at http://homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading03.html (last visited Oct 13, 2015).
[4] Berni Dwan, *Identity theft*, 2004 Computer Fraud & Security 14-17 (2004).
[5] Vivek Tripathi, Cyber Laws India Cyberlawsindia.net, http://www.cyberlawsindia.net/index1.html (last visited Oct 13, 2015).

Security Number. Through this number, an individual avails government schemes and record of the entire database pertaining to the individual revolves around his social security number. In such circumstances, a leakage of this number to identity thieves can have serious irreparable repercussions unless such miscreant is tracked down. As per the India Risk Survey Report, 2014, there has been a 11% increase in ransom ware and identity theft in India, followed by a 9% increase in Phishing attacks.[6] In 2013, India had been ranked amongst the top 5 countries with the most number of cybercrimes.[7] Despite high level of cybercrimes, there is a startling level of low conviction rate in India.[8] With around 354 Million internet users in India,[9] the fact of rising number of cybercrimes and low conviction rates is problematic. Therefore, the present laws catering to the cybercrime need to be critically analyzed, to understand whether the law or its implementation has certain lacunae which have led to this problem.

The research question is whether and to what extent are the Indian laws pertaining to identity theft sufficient to cater to the present requirement and whether the implementation mechanism of the laws is in synchrony with the legislations.

The researcher would go into the intricacies of the crime of identity theft committed through electronic resources specially computer and internet. The country of study would be India and the researcher would analyze various legal provisions in the Indian Penal Code, 1860 and primarily in the Information Technology (Amendment) Act, of 2008 aimed at civil and criminal liability of an identity thief and the remedies available to the victim. The shortcomings (if any) would be exposed and certain reform measures would be suggested.

[6] India Risk Survey, 2014, (1 ed. 2014), http://www.ficci.com/Sedocument/20276/report-India-Risk-Survey-2014.pdf (last visited Oct 13, 2015).

[7] *Ibid*

[8] Rajlakshmi Wagh, *Comparative Analysis of Trends of Cyber Crime Laws in USA and India*, 2 International Journal of Advanced Computer Science and Information Technology pp. 42-50 (2013), http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-160 (last visited Oct 13, 2015).

[9] Dazeinfo, Internet Users In India: 354M, 60% Access From Mobile [REPORT] - Dazeinfo (2015), available at http://dazeinfo.com/2015/09/05/internet-users-in-india-number-mobile-iamai/ (last visited Oct 13, 2015).

WHAT CONSTITUTES IDENTITY

In general parlance, identity of an individual is a collection of unique and stable characteristics associated with the person which distinguishes him/her from others.[10] Each individual, even two similar looking individuals have a unique identity. In legal context, identity encompasses the recognition aspect of an individual as per the government records through birth registration, voter ID, driving license, etc. It constitutes the name, citizenship, address, physically distinguishing feature (a scar or mole), photograph, and blood group information. This can help the authorities to keep a track of the people residing or visiting the territory.

Identity for the purpose of Identity theft crimes can range from Social Security Numbers to details of credit card account. It includes any such information which can be used by the criminal to take over the victim's identity to commit myriad crimes.[11] Section 66 C of the Information Technology (Amendment) Act, 2008 includes electronic signatures and password into the meaning of identity.

IDENTITY THEFT – MEANING AND THE WAYS IN WHICH THE CRIME CAN BE COMMITTED

Identity theft includes usage of fraud or cheating methods to procure someone's identity information so as to use such information to access resources or to obtain credit and other benefits in the victim's name.[12]

Although identity theft was possible even before the advent of the internet era wherein traditional methods of physical crimes were used to perpetrate identity theft, excessive

[10] THE EVOLUTIONAL VIEW OF THE TYPES OF IDENTITY TH EFTS AND ONLINE FRAUDS IN THE ERA OF THE INTERNET, Internet Journal of Criminology © (2011), available at www.internetjournalofcriminology.com/wang_huang_the_evolutional_view_of_the_types_of_identity_thefts_and_online_frauds_in_the_era_of_internet_ijc_oct_2011.pdf (last visited Oct 13, 2015).

[11] Siddharth Buxy, IDENTITY THEFT ON THE INTERNET: SUGGESTIONS FOR THE INFORMATION TECHNOLOGY ACT (1 ed.), http://thegiga.in/LinkClick.aspx?fileticket=KX1_Imk_gDs%3D&tabid=589 (last visited Oct 13, 2015).

[12] LARRY J. SIEGEL, E-STUDY GUIDE FOR: CRIMINOLOGY: THEORIES, PATTERNS, AND TYPOLOGIES (11 ED. 2014).

dependence on internet has led to the comparatively less laborious identity theft as we understand it today. Earlier, some of the methods used to illegally get hold of an individual's personal identity information were stealing personal mails like bill statements from the letter box, bribing or deceiving the employer or relevant authorities who possess their employee's/ client's personal information or purchasing the stolen identity cards from the dealers associated with this illicit trade. Another method was dumpster diving where identity information is gathered from the trash dumped by individuals consisting of documents like bank statements, cheque, bills, and storage devices or discarded credit cards.[13] Information was also accessed by the victim directly by the fraudster pretending to be a customer service representative, a survey researcher, etc. Though these methods are still prevalent, they were quite risky, cumbersome and had a high chance of the culprit being traced quickly.

Technology has made the whole process much easier, while tracking it much difficult or sometimes even impossible. Internet and online transactions provide a kind of anonymity and privacy to an individual.[14] He/she can live a life of multiple identities through e-mail ids and passwords, which do not require physical verification of the details of the actual person. Although such conduct is illegal under Section 464 of the IPC (making a false electronic document) and punishable under Section 465 of the same code,[15] it is generally not brought under the notice of the police unless some other crime is reported of being committed using such false identity. Hence this practice is widely prevalent and provides a broader scope of committing crime with less chances of detection.

The crime of identity theft consists of two steps which may or may not be committed by the same person, namely:[16]

1). Wrongful collection or procurement of personal identity information of an individual.

2). Wrongful use of such information with an intention of causing legal harm to that person.

The first step of fraudulently obtaining personal identification information can be done in several ways. It can be done by the thief who fraudulently uses such data himself or buys the stolen identity from dealers in such illegal trade. Here too, coming in contact with such

[13] *Supra Note 10*

[14] *ibid*

[15] Rohas Nagpal, Is it legal to open a Facebook account in a fake name? | Facebook Law (India) Facebooklaw.in (2013), http://www.facebooklaw.in/is-it-legal-to-open-a-facebook-account-in-a-fake-name/ (last visited Oct 13, 2015).

[16] *Supra Note 10*

traders becomes easier through the internet. As the researcher is focusing on computer aided ID theft, techniques of procuring personal data from electronic devices are as follows:

1). Hacking : It is a method through which malware like computer viruses or worms are used to divert information to the hackers who decrypt it and then either use it themselves or sell it to others to commit fraud using such information. Such attacks can be done in the garb of infected links, free software download, signing in through Facebook account or where there is no proper firewall protection or strong password to protect networks or computers as such.[17]

2). Phishing: The fraudster may send an e-mail with a link of a fake website which may resemble some authentic link to, say a bank site, where personal information and account information will be asked.[18] The reasons for seeking such information may be for keeping the customer's information up to date for better services by the bank, or claiming that the failure of giving such information would amount to suspension of the account.

3). Pharming : It is similar to Phishing but in this, clicking on the authentic link of the bank website would redirect the websites traffic to a fake site even if the user has entered a valid internet address. Pharming is done by installing malicious code either in the personal computer or in a server. [19] Hence, it can target various users at the same time. It happens without the consent or knowledge of the victim and is often called "*Phishing without a lure*". [20]

4). Nigeria 419 Scam: This method is target specific where the fraudster sends an e-mail as a rich family member of a dead African millionaire wanting to use the victim's bank account to transfer some money on the pretext that it is difficult to access it due to the political turmoil in his country, in return of a huge sum of money as payment for the transfer.[21] Another of its kind is intimating the victim of a huge lottery amount won by him amongst thousands of

[17] Privacymatters.com, Computer Hacking and Identity Theft | PrivacyMatters.com, available at www.privacymatters.com/identity-theft-information/identity-theft-computer-hacking.aspx (last visited Oct 13, 2015).

[18] Neeraj Aarora, Identity Theft or Identity Fraud | A Platform to discuss & analyse Financial and Cyber ForensicsA Platform to discuss & analyse Financial and Cyber Forensics Neerajaarora.com (2009), available at www.neerajaarora.com/identity-theft-or-identity-fraud/ (last visited Oct 13, 2015).

[19] SearchSecurity, What is pharming? - Definition from WhatIs.com (2007), available at http://searchsecurity.techtarget.com/definition/pharming (last visited Oct 13, 2015).

[20] *ibid*

[21] Australian Competition and Consumer Commission, Nigerian scams, https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams (last visited Oct 13, 2015).

accounts and asking for the account details to transfer such lottery amount. Such details once given by the gullible user are used to steal their funds.

5). Skimming: This employs various devices stealthily attached to the ATM machines or any other machines where the credit or debit card is put to use. These stealth devices fit on the original machines and have a magnetic card reader which a pin hole camera to shoot the victims movement on the machine while he/she enters the PIN. Some sophisticated skimming devices generate an automatic message received by the thief, each time a person swipes his card.[22]

6). Vishing: In this, the fraudster calls the victim by posing to be a bank representative or a call center employee, thereby tricking the victim to disclose crucial information about the identity.

Some other forms of methods include online frauds like advertising/ advertisement click frauds and business transaction fraud involving online payment through unsecured gateways.[23]

After the initial step of illegal personal identity information collection is completed, various crimes aimed at achieving economic enrichment like withdrawing money from the existing account or applying for new bank loans, credits cards, benefit from certain government schemes in the name of the stolen identity are committed. This creation of new means of identification using an existing identity of the victim is called breeder identification.[24] Such thief might not have been able to avail these facilities if he had applied in his real name. Sometimes, graver crimes other than impersonation, forgery, cheating, immigration fraud, etc. can be committed. The stolen identity information can be used to procure illegal weapons or bomb parts by the terrorists to dodge the authorities which can subject the victim to stricter laws. In such a case, proving the victim's innocence becomes very difficult unless the fact of stolen identity information comes to the notice of the victim before it is used in furtherance of terrorist activities and he reports it to the police. This again is not possible if such personal information is stealthily accessed through a computer, in which case no trace or sign of theft can be gauged before the information is actually used for illegal purposes.

[22] Krebsonsecurity.com, Would You Have Spotted the Fraud? — Krebs on Security (2011), available at http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/ (last visited Oct 13, 2015).
[23] *Supra Note 9*
[24] *ibid*

LAWS GOVERNING IDENTITY THEFT IN INDIA

India does not have a standalone legislation for identity theft but the Information Technology (Amendment) Act,2008 along with several provisions in the Indian Penal Code,[25]1860 are used to cater to this crime. As identity theft has features of both theft and fraud, the basic provisions of fraud, forgery and cheating by impersonation, etc as provided in the IPC are often invoked along with those of the IT Act.

WHETHER IDENTITY THEFT IS THEFT WITHIN THE MEANING OF IPC, 1860

Although by its name, identity theft is a kind of theft of specific kind involving user data, it is not governed by Section 378 (theft) of the IPC.[26] This is because, it caters to only movable property or such property which is capable of being severed from the earth, and is tangible in nature (Section 22 of IPC). Electricity has been included within the ambit of theft but in the case of **Avtar Singh v. State of Punjab**,[27] the Supreme Court held that it is because of the Section 39 of the Electricity Act and there was no intention of widening the scope of Section 378 of the IPC. Hence, although identity information is in the form of binary data signals of zeros and ones, governed by streams of electronic waves like electricity, Section 378 cannot be read to include data or identity theft.[28]

PROVISIONS OF THE IPC THAT CAN BE USED FOR IDENTITY THEFT

Certain provisions in the IPC, like forgery and fraud, which earlier governed such crimes with respect to false documents, were amended by the Information Technology Act, 2000 to include electronic record. Hence, the ambit of such crimes was widened to include computer data related crimes as well. Hence forgery(Section 464), making false documents(Section 465), forgery for purpose of cheating (Section 468), forgery for purpose of harming

[25] Hereinafter referred to as IPC.
[26] Padala Rama Reddy, Indian Penal Code, 1860 196 (16 ed. 2014).
[27] Avtar Singh v. State of Punjab AIR1965SC666
[28] Robin George, Data Theft in Cyber Space Legalserviceindia.com (2008), available at www.legalserviceindia.com/article/l267-Data-Theft-in-Cyber-Space.html (last visited Oct 14, 2015).

reputation(Section 469), using as genuine a forged document (Section 471) and possession of a document known to be forged and intending to use it as genuine (Section 474) can be coupled with those in the IT Act. For instance, Section 468 and Section 471 can be triggered when a person forges a website in nature of electronic record in order to lure the victims into divulging their sensitive information with the intention to cheat them. Further, Section 419 can be used in cases where the accused has used the personal identity information of the victim and impersonates such victim to commit fraud or cheating. Section 420 can be used if *"anything capable of being converted into a valuable security"* within the meaning of the act is read to include unique identification information of an individual.

Further, the Expert Committee on Amendments to the IT Act, 2000 had recommended certain amendments in the IPC to include Section 417 A which would provide up to three years of punishment for cheating using any unique identification feature of another person.[29] It also made cheating by impersonation by way of a network or computer resource punishable with up to five years imprisonment and a fine, under Section 419 A.[30] These recommendations have not been incorporated into the IPC as yet, but would have provided a more comprehensive law on identity theft.

PROVISIONS IN THE INFORMATION TECHNOLOGY ACT, 2000

The IT Act, 2000 is the main legislation in India governing cybercrimes. Although, its aim was to mainly recognize e- commerce in India and it did not define cybercrimes as such.[31] Before its amendment in 2008, Section 43 of the Act could be used to impose civil liability by way of compensation not exceeding one Crore for unauthorized access to a computer system or network (Subsection a) and for providing assistance to facilitate such illegal act (Subsection g).[32] Section 66 of the Act only pertained to cybercrime of hacking wherein some destruction, deletion, alteration or reduction in the value of computer resource attracted penal sanctions.[33] If a person obtained identity information from the computer stealthily without

[29] *Supra Note 17)*
[30] *ibid*
[31] Sanjay Pandey, Curbing Cyber Crime: A Critique of Information technology Act 2000 and IT Act Amendment 2008 (1 ed.), http://www.softcell.com/pdf/IT-Act-Paper.pdf (last visited Oct 14, 2015).
[32] MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department), THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000) (2000).
[33] *ibid*

causing any changes in it whatsoever, this provision could not be used. The term identity theft itself was used for the first time in the amended version of the IT Act in 2008.[34] Section 66 criminalizes any fraudulent and dishonest conduct with respect to Section 43 of the same Act.[35] Section 66 (A) which is now held to be unconstitutional, covered the crimes of Phishing. Section 66 B pertains to dishonestly receiving any stolen computer resource. Section 66 C specifically provides for punishment for identity theft and is the only place where it is defined. Section 66 D on the other hand was inserted to punish cheating by impersonation using computer resources. This provision can be seen to be similar to the Section 419 A) recommendations of the expert committee as mentioned earlier.[36] Several other provisions inserted in the amendment include punishment for violation of privacy and for cyber terrorism. Women and children have also been provided protection under Section 67 A and 67 B of the Act. Further, stronger laws have been formulated with respect to protection of "sensitive personal data" in the hands of the intermediaries and service providers (body corporate) thereby ensuring data protection and privacy. Only exceptional cases where such data can be revealed is to an agency authorized by the State or Central government for surveillance, monitoring or interception, under Section 69 of the IT Act. The ambit of sensitive personal data is defined by the IT Rules, 2011 to mean password, financial information, physical physiological and mental health condition, sexual orientation, medical record and history, and biometric information.[37]

Hence, depending upon the method using which identity theft has been committed, the aforementioned laws can be applied.

[34] MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department), the Information Technology (Amendment) Act, 2008 (2009).
[35] *ibid*
[36] *Supra Note 29*
[37] Amber Gupta, Data Privacy in India and data theft Slideshare.net (2013), available at www.slideshare.net/AmberGupta6/data-privacy-in-india-and-data-theft (last visited Oct 14, 2015).

INSTANCES OF IDENTITY THEFT AND THE LOSS CAUSED TO THE VICTIMS – WITH A FOCUS ON CASES THAT OCCURRED IN INDIA

Identity theft cases are on a rise world over. In U.S. alone, about 15 Million residents have their identities used fraudulently every year, with total loss of about $50 Billion. [38] About 100 Million additional Americans have their personal data at risk when records maintained in Government and corporate database is lost or stolen.[39] Similarly in India, as per the research finding of a company, one out of four is a victim of identity theft and such cases have risen by a 13% since 2011.[40] As per the Microsoft's Third Annual Computing Safer Index, at least 20% of Indians have fallen prey to phishing attacks and identity theft has caused loss of around Rs. 7500 on an average.[41] The numbers shown in this Survey is quite large if we consider the fact that the total internet users in India are around 19.9% of the entire population.[42]

SOME FAMOUS CASES OF IDENTITY THEFT ACROSS THE WORLD

Due to their fame and presence in the social circle, getting personal identity information of celebrities is comparatively easier. This is because, much is known about the life of celebrities and when most of the data is protected by a password which can be changed easily by guessing the answer to the security question. Hence, they are an easy target of Identity theft. First in this list is Michael Bloomberg, the famous American Businessman and owner of the Bloomberg LP Company. A criminal used his information to withdraw a four figure amount from his bank account through an online transaction and another criminal used a

[38] Rob Douglas, Identity Theft Statistics: 15 million victims a year | www.IdentityTheft.info Identitytheft.info, available at www.identitytheft.info/victims.aspx (last visited Oct 14, 2015).

[39] *ibid*

[40] Silicon India, Identity Theft: a Major Threat to India (2013), available at www.siliconindia.com/finance/news/Identity-Theft-a-Major-Threat-to-India-nid-143825.html (last visited Oct 14, 2015).

[41] Timesofindia-economictimes, Identity theft costs Indians Rs 7,500 on an average: Microsoft (2014), available at http://articles.economictimes.indiatimes.com/2014-02-11/news/47235749_1_identity-theft-microsoft-new-internet-users (last visited Oct 14, 2015).

[42] Internetlivestats.com, India Internet Users - Internet Live Stats (2015), available at www.internetlivestats.com/internet-users/india/ (last visited Oct 14, 2015).

forged cheque in Bloomberg's name to transfer $ 190,000 into his own account.[43] Similarly, a cybercriminal hacked into the Social Security number, date of birth and credit card information of golfer Tiger Woods and undertook an online transaction worth $ 17,000. Similar identity thefts were faced by actor Will Smith and singer Whitney Houston.[44] In India, it was the government's Income Tax Portal which became the target. In two distinct cases, a hacker from Hyderabad, hacked into industrialist Anil Ambani's income tax returns account while another from Noida accessed Shah Rukh Khan, Mahendra Singh Dhoni and Sachin Tendulkar's income tax details.[45]

Several other large scale identity theft instances in India include the RBI Phishing Scam, ICC World Cup, 2011 scam and the password phishing scam targeting Google email account holders.[46] As phishing scams have become common ways of committing identity theft in India, the Delhi High Court, in the landmark case of **NASSCOM v. Ajay Sood and Ors**,[47] declared phishing on the internet as an illegal act against which damages could be claimed. This case was decided in 2005 when there were no specific laws punishing phishing. The court set precedence and called phishing as misrepresentation in course of trade, leading to confusion as to source of origin of e-mail and not only causing harm to the intended victim but also tarnishing the image of the person whose identity is misused.[48]

IMPACT OF IDENTITY THEFT ON THE VICTIM

The impact of an identity theft on a victim depends on the extent to which the identity has been used to commit further crimes. The stolen identity can be used to either cause economic loss to the victim of such theft or to defame by creating fake social media profile using the

[43] Reagan Gavin Rasquinha, *From Will Smith to Tiger Woods: Famous folk who were victims of identity theft*, The Times of India, 2015, http://timesofindia.indiatimes.com/entertainment/english/hollywood/news/From-Will-Smith-to-Tiger-Woods-Famous-folk-who-were-victims-of-identity-theft/articleshow/48915181.cms (last visited Oct 14, 2015).

[44] *ibid*

[45] Abhijit Sathe, *Sachin, Shah Rukh, Salman and Dhoni's tax accounts hacked*, Mumbai Mirrir, 2013, available at http://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/Sachin-Shah-Rukh-SalmanDhoni/articleshow/23078943.cms (last visited Oct 14, 2015).

[46] *Supra Note 10*

[47] NASSCOM v. Ajay Sood and Ors. 119 (2005) DLT 596

[48] Cyberralegalservices.com, Case Studies, available at www.cyberralegalservices.com/detail-casestudies.php (last visited Oct 14, 2015).

information. In the first case there is measurable monetary damage caused to the victim but in both of the above cases, there is an implicit and immeasurable loss caused to the reputation.

Firstly, where the personal information of the victim is used to commit economic offences, the default in payment of say bank loans or credit card dues, etc. transacted by the impersonator is duly noted by the credit reporting agencies. Mostly, the victim comes to know about the identity theft when he/she checks the credit history at the time of applying for a loan, or when the victim's valid credit card account is frozen by the bank due to default in payment of a sum that the victim never withdrew. The real trauma that the victim faces begins after the identity theft has been perpetrated, not because of the original crime (whose cost is somewhat recovered as compensation in court) but because of the victim has to get his/her credit restored and his/her name cleared in the credit records.[49] This is a very arduous process, the cost (in terms of time spent to go through the entire process) of which is not considered by the courts at all. Hence, this can be called the implicit cost borne entirely by the victim.

In the Indian context, Credit Information Bureau (India) Ltd. (CIBIL) was the first credit bureau in India.[50] Other bureaus that came subsequently include Equifax and Experian. These organizations keep a record of the credit worthiness of the borrower.[51] When a lender gives a false report of the borrower to the bureau or when an identity thief takes loans or opens up accounts in the name of the victim and thereby defaults in payment, the genuine identity holder can be denied credit. Even when a victim wins his case and proves that he is a victim of identity theft, he himself has to approach the credit bureau to get the records updated.[52] No compensation is paid to the victim for the loss caused due to false credit reporting by lenders (like banks) or for delay in correction of credit information by the credit bureau. In India, there is no law making the credit bureaus liable or accountable for the mistake or negligence in the credit report of an individual. India needs a law which is in line with the Fair Credit Reporting Act in the U.S.A which provides for strict penalties for faulty reporting or non-

[49] Dr. P. Arunachalam, *Economic Impact of Identity Theft in India: Lessons from Western Countries*, 12 International Journal of Marketing and Trade Policy (2011).

[50] Vishal Ingole, *Credit Data Bureaus– Why India Needs More Players*, Business Insider India, 2014, available at www.businessinsider.in/Credit-Data-Bureaus-Why-India-Needs-More-Players/articleshow/39298151.cms (last visited Oct 14, 2015).

[51] *ibid*

[52] Jeanine Skowronski, Identity-Theft Victims Pay High Price When Their Data Get Stolen | Bankrate.com Bankrate.com (2015), http://www.bankrate.com/finance/credit/high-cost-of-identity-theft.aspx (last visited Oct 14, 2015).

maintenance of the standards,[53] to protect the interests of the victim and grant speedy redressal.

The above solution can be implemented in case of pure economic crimes committed by the identity thief when the victim is able to prove his/her innocence without much loss of social reputation after getting arrested for the same. In a situation where the stolen identity information is used to commit graver offences like creating a fake social media profile of the victim with pornographic content or using the victim's identity to commit other cyber offences, the damage is more and much difficult and time consuming to set right. One such unfortunate incident happened with Simon Bunce in UK, where an identity theft landed him in the list of internet pedophiles and led to his arrest in the Operation Ore conducted by the U.K. police.[54] The repercussions of his arrest were severe. He was dismissed by his employer from a £120,000 a year job and his family disowned him. The computer technicians took several months to examine his computer and storage devices. In the meantime, Simon himself started investigating the matter in order to collect proof of his innocence with the aid of the Freedom of information Act applicable in the U.S. His credit card details had been used in a child pornographic website by the identity thief who hacked the details from the online shopping payment gateway "Landslide", based in U.S., which was frequented by the victim. He was able to prove that he was in a restaurant in London while his credit card details had been used by a person whose IP Address was traced to Jakarta, Indonesia. It took another six months for Simon to get a new job paying him three- fourth amount less than what his earlier job earned him and much longer time to remove the blemishes from his tarnished reputation.[55]

These instances can be applied in India as well, due to the universal *modus operandi* of the identity thieves. Hence, an identity theft victim in some cases does not only suffer economic losses that can be rectified by compensation, certain latent costs as mentioned above are also suffered which can only be reduced by efficiency of the laws and co-operation of the authorities.

[53] Harsh Roongta, High time for India to have a fair credit reporting law Business-standard.com (2015), available at www.business-standard.com/article/pf/high-time-for-india-to-have-a-fair-credit-reporting-law-115032900698_1.html (last visited Oct 14, 2015).

[54] Marc Sigsworth, *'I was falsely branded a paedophile'*, BBC News, 2008, available at http://news.bbc.co.uk/2/hi/uk_news/magazine/7326736.stm (last visited Oct 14, 2015).

[55] *ibid*

LACUNAE IN THE INDIAN LAWS ON IDENTITY THEFT AND ITS IMPLEMENTATION

The Information Technology Act, 2000 subsequent to its amendment in 2008 has gone a long way in protecting data and personal information of an individual from being misused. Still, there are certain aspects of the legislation and laws on identity theft that require clarity or changes. Firstly, Section 66 C of the amended Act protects "unique identification feature", the meaning of which has not been specified anywhere in the Act. The Information Technology Rules, 2011 has defined "sensitive personal information" which need to be protected by the intermediaries. But it would be too farfetched to decipher unique identification feature to mean sensitive personal information unless interpreted by the judiciary or expressly provided by a legislation.

Secondly, although the IT Act is applicable to any individual who is involved in identity theft involving any computer resource based in India, the jurisdictional issues still cannot be reconciled. When the accused is a non-Indian citizen, the country of his citizenship has dissimilar laws pertaining to identity theft and has not signed an extradition treaty with India, arrest of such accused cannot be undertaken.[56]

Thirdly, considering the compensation awarded to the victim, the Act is inadequate. Under Section 43of the IT Act, the compensation awarded has an upper limit of 1 Crore and if loss of data is caused by body corporate, the cap is 5 Crore. A victim might suffer larger loss than this amount, but that aspect is disregarded. Further, as per Section 47 of the Act, the Adjudicating Officer looking into the cases where claims are below 5 Crore has to consider only into tangible/quantifiable loss caused to the victim while awarding compensation. As discussed earlier in the paper, there is huge amount of mental trauma and hardship that the victim faces as an aftermath of the crime depending upon the subsequent crime to which the unique identification information is put to use. It takes much time and resources to regain the lost reputation or to get the credit report corrected, which should also be accounted for while awarding compensation.

[56] Prashant Mali et al., Data Theft and The IT Act, 2000 of India | Daily Host News Dailyhostnews.com (2013), available at www.dailyhostnews.com/data-theft-and-the-it-act-2000-of-india (last visited Oct 14, 2015).

Fourthly, the fine provided for identity theft under Section 66 C of the Act is up to I Lakh only. Identity theft is a larger umbrella under which crimes of different intensity can be perpetrated. An identity thief can cause loss of property to a single person worth some thousand rupees or to a large population where loss may amount to millions. In both the cases, a minimal token fine not exceeding one lakh would be imposed. Further, the other Sections of the Indian Penal Code along with which Section 66 C of the IT Act may be clubbed, do not mention the limit (upper or lower) of fine or the manner in which it should be tabulated, thus leaving it to the discretion of the judge.

Lastly, laws are meant to serve a dual purpose of prevention of a crime and deterrence.[57] Pre-emption and thereby prevention of identity theft is not possible. The deterrence effect can be created in case of this crime where generally a certain amount of premeditation or pre thought is invested before its commission. This can be done by imposing stricter punishment and/or fines. At present, the IT Act makes identity theft a cognizable, bailable and compoundable offence. Section 77 A provides for offences committed under Section 66 C to be compoundable. Further, a three year imprisonment term is meager and will not serve the purpose of deterrence. By making the provision bailable, it might provide an opportunity to the accused might interfere with the investigation of the crime by the cyber cell by tampering with his digital footprints and evidence of his crime.

PROBLEMS IN IMPLEMENTATION OF THE LAWS

Although the occurrence of cybercrimes is burgeoning year after year, the conviction rate in India is dismally low.[58] As against 3682 complaints, 1600 out of the accused have been arrested and merely 7 out of them have been convicted as per 2013 data.[59]This might be due to improper implementation of the existing rules or an insufficiency in the infrastructure required in implementing the laws. Firstly, there is a dearth of police personnel specialized in

[57] The purpose of Criminal Punishment, (1 ed. 2004), http://www.sagepub.com/sites/default/files/upm-binaries/5144_Banks_II_Proof_Chapter_5.pdf (last visited Oct 14, 2015).

[58] Rajlakshmi Wagh, *Comparative Analysis of Trends of Cyber Crime Laws in USA and India*, 2 International Journal of Advanced Computer Science and Information Technology pp. 42-50 (2013), http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-160 (last visited Oct 14, 2015).

[59] *ibid*

dealing with cybercrime cases. With time, due to technological advancement, new forms of encryption technology are used by the cyber criminals, which is difficult to decipher owing to the limited resources of the authorities. This delays the entire process, sometimes leading to releasing the accused due to lack of proof. In U.S. some judicial pronouncements have given the power to the police to ask the cybercriminal to decrypt the digital evidence in return of some imprisonment concessions, but it has not been deployed often.[60] Also, the number of cyber labs in India is eight till date,[61] which are overburdened due to the numerous cybercrime cases. Lastly, one of the reasons for low rate of conviction or reporting may be because of non-registration of cybercrime complaints by the police.[62] This issue should also be looked into. These shortcomings can be overcome by increasing the number of vacancies for skilled police officers by the government and deploying more funds to update to the latest technology which can aid in the present day requirement of confronting a cybercriminal.

CONCLUSION AND RECOMMENDATIONS FROM CROSS CULTURAL LEGAL SYSTEMS

Mechanism and laws to punish identity thieves should be taken care of by the legislature. But it is also important that the data theft is prevented altogether by implementing stricter data protection laws. The major sources from which sensitive identity information can be accessed by cyber criminals are the service providers which are basically BPO and IT companies having the personal database of people around the world. Although, the data protection laws in India are not very strong at present but the proposed Personal Data Protection Bill is a positive step towards implementing stricter data protection laws.[63] It is based on the European

[60] Neeraj Aarora, GOONDA ACT- INEFFICACY OF POLICE TO CONQUER INTERNET CRIME | A Platform to discuss & analyse Financial and Cyber Forensics A Platform to discuss & analyse Financial and Cyber Forensics Neerajaarora.com (2014), available at www.neerajaarora.com/goonda-act-inefficacy-of-police-to-conquer-internet-crime/ (last visited Oct 14, 2015).

[61] Dsci.in, Cyber Labs | Data Security Council of India, available at www.dsci.in/taxonomypage/283 (last visited Oct 14, 2015).

[62] *Supra Note 59*

[63] Data Protection Act in India with Compared to the European Union Countries, 11 International Journal of Electrical & Computer Sciences (2011), available at www.ijens.org/Vol_11_I_06/112206-7474-IJECS-IJENS.pdf.

Union Data Privacy Directive of 1996 and applies to both the government as well as the private companies.[64]

Following are the recommendations that can be implemented in India to make the laws regarding identity theft more effective.

- Making amendment to the present laws for imposing stricter punishment for aggravated forms of identity theft. The laws can be made victim friendly such that he/she is able to recover from the loss caused and providing as much restitution as possible. India can look into the laws in U.S. which has incorporated the above ideas in the form of two legislations.[65]Therefore, the victim must be given support, both for the immediate loss caused by Identity theft and for the aftermath of such crime.
- In India, various police departments have their own cyber-crime units where police officers are not well trained and find it difficult to deal with cybercrimes. Due to their lack of expertise in this area, either the cybercrimes remain unreported or prone to improper investigation.[66] This issue has been brought to the honorable Supreme Court's notice in several PILs. Special agency independent of the police (like the National Hi- Tech Crime Unit in U.K.),[67] or a different training academy must be established in India which can help the local police department to investigate the cybercrime.
- Cybercrime which happens at a large scale is generally transnational in nature. Various countries should co-operate using multilateral treaties in order to have basic uniformity in terms of sharing cybercrime information. One such example is the Indo-American alert, watch and warn network which deals with cases falling in Indo-American jurisdiction.[68]
- In order to prevent or minimize threat of identity theft, the biological aspect of identity verification (biometric) like fingerprint, voiceprint, iris scan and hand

[64] *ibid*

[65] The *Identity Theft Penalty Enhancement Act*, 2004& The *Identity Theft Enforcement and Restitution Act* of 2008

[66] B Singh, Regulations and Guidelines for Effective Investigation of Cyber Crimes in India | Centre of Excellence for Cyber Security Research and Development in India (CECSRDI) Perry4law.org (2013), available at http://perry4law.org/cecsrdi/?p=302 (last visited Oct 14, 2015).

[67] F Cassim, *Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?*, 18 Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad 68 (2015).

[68] Cyber Law Trends and Developments of India 2013, (1 ed. 2013), http://ptlb.in/ccici/wp-content/uploads/2013/12/Cyber-Law-Trends-And-Developments-Of-India-2013.pdf (last visited Oct 14, 2015).

geometry, etc. should be used where ever there is an online financial transactions or email account login.[69] Such unique information can be collected and stored at the time of registration or signing up with the websites.

- Lastly, the government needs to create awareness amongst consumers with respect to ways of protecting personal information and safe internet practices. Further they need to be educated about their rights and redressal mechanism available to them in case of an identity theft. To minimize the harm and early detection of identity theft, individuals should keep a track of their credit report.

It is submitted that a careful perusal of the identity theft practices and laws in India gives an impression that by slight modification, as suggested, to the existing laws and its effective implementation, instances of identity theft can be controlled. The loss caused to the victim can be mitigated as far as possible and by holding the intermediaries accountable for the data that they hold, data privacy can be upheld. The law and its implementation does not seem to overlap. The implementation aspect lags behind the legislations, due to which the true efficiency of the present laws is not being achieved.

[69] *Supra Note 9*