How to Cite:
Charaya, S., & Pathak, D. N. (2022). Issues and challenges with changing perspective of time in cyber tort. *International Journal of Health Sciences*, *6*(S2), 13662–13672. https://doi.org/10.53730/ijhs.v6nS2.8736

Issues and challenges with changing perspective of time in Cyber tort

Shivam Charaya
Student of 10th semester BA.LLB at Law College Dehradun, Uttaranchal University Dehradun, 248007, Uttarakhand, India
Corresponding author email: shivamcharaya012@gmail.com

Dr. Deependra Nath Pathak
Asst. Professor at Law College Dehradun, Uttaranchal University Dehradun, 248007, Uttarakhand, India
Email: deependra4all@gmail.com

***Abstract*---**Private details such as usernames, Cybercriminals often collect the victim's identification numbers, credit card information, and social security number in order to conduct fraud in the name of the other person. These confidential details may be used for a number of illegal purposes, including requesting loans, making online purchases, and getting entry to the victim's financial and health details. The use of an individual's identity for wrongful purposes like fraud and other getting their information illegally is known as identity theft. It can range from using their surname, social security number, or credit card details, against their authorization. The term "identity theft" was created in 1964. Both in the United Kingdom and the United States, identity fraud is now legally characterized by loss of personally identifiable information. Identity fraud is the fraudulent use of some other particular personality to get financial or other rewards.

***Keywords*---**identity theft, personal information, password, credit card.

Introduction

The first and foremost step taken was defining cybercrime. As per the FBI "Offenses perpetrated against individuals or organizations with malice to deliberately tarnish the original holder's image or cause any type of harm that can either be bodily or psychological, explicitly or implicitly, with the use of contemporary technology, which in today's times can be the internet or other modes of telecommunication like email, boards, chat room) and different

text messages like SMS and MMS. It is a recent crime that entails the use of prohibited substances.

Any digital communication machine or information system can be used to conduct activities in cyberspace. Alternatively, the internet can act both as a tool or a target. Cyberspace can be claimed to be a virtual environment in which a space is created with no boundaries since communication takes occur across a computer network. It's basically the creation of a geographical place and is accessible to anyone with internet access anywhere in the world.[1] Cybercrime is on the rise in modern times, as people become more reliant on computers, the internet, and related technologies, as well as the digitization of different services. It's turning into a major threat that has to be addressed immediately. Thereby in a world full of technological advancement, the use of internet and other nspired software , hardware, and technology have both detrimental and beneficial aspects to them. Identity theft in internet is one such crime. Identity theft is a type of cybercrime whereby a person having identity is taken in to the process to achieve an illicit financial upscale or deceiving people, and in some situations, it can put the victim's personal safety at risk.[2]

Concept of Identity Theft

When identity theft occurs in cyberspace, it is referred to as the identity theft on web or cyberspace data theft. Identity theft is a serious problem in today's digital world. The characteristic of identity theft and its breadth, from individuals to transnational companies, are discussed in this essay. It also looks at who the players are and why they commit such crimes.[3] Victims and the impacts of identity theft are highlighted, as well as the motivations of perpetrators, ranging from single-actor actions to organized crime tactics. Rather than using forceful access into a system, thought was given to the weaknesses of technologies that are breached by identity fraud and how the design of a network's weaknesses are abused. The combination of crypto-currencies and dark web activity is highlighted as posing challenges in preventing perpetrators from being discovered. There are suggestions for more research into safeguarding networked systems and forensic accounting. [4]

The term of the crime is a little misleading because when possession is taken, the sufferer is dispossessed, however when a person's identity is taken, the victim is not dispossessed. The identity of a person, whether living or dead, is defined as and includes their detailed information , such as their Surname, personal details, user id, bank details , IT return forms, medical insurance information, plus additional accounts.[5]

---

[1] Halder and Jaishankar, Cyber Crime and Victimization of Women: Laws, rights and Regulations, 2011, ISBN no. 978-1-60960-830-9

[2] Dr SR Myneni, Information technology law (cyber laws), 1 st Edition, Asia law house, Page no. 33.

[3] Easttom and Taylor (2011).

[4] https://www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017-11571735243602.html.

[5] National Crime Record Bureau, Crime Report 2018, Page no.- xiii

Identity theft and stealing personal information are terms that are sometimes used interchangeably to define numerous sorts of violence that someone commits unjustly gets and exploits another man's individual data in certain manner including fraud or deception, usually for financial benefit. Hacking passwords, phishing, malicious websites, distributed denial of service, suspension of deliverydata theft, malware installation, spyware, e-mail/SMS spoofing are just a few of the ways this crime is done, and new techniques are emerging every day.[6] These crimes differ from traditional crimes in terms of reporting, determining jurisdiction, investigation, and trial. To combat such crimes, law enforcement organizations must have industry induced information and competence in the operation of computers and the internet. This will allow for a swift trial and just penalty for the criminals. Such criminality is becoming more common, resulting in significant financial losses for private enterprises and the government in India and around the world.[7]

As per the Norton Cyber Security Insights Report 2016, cybercrime affects 49 percent of the nations internet demographic, or maybe more than 115 million Indians , ultimately, ranking the country second with respect to the suffers of fraud.[8] With the expanding use of cloud computing, that allows various users entry to information saved, the saved information is becoming more exposed to cybercrime. These patterns indicate that an effective and comprehensive legal redress system, as well as preventive measures, are required to decrease generational violence and aid India's transformation into a trillion-dollar economy.

Identity Theft as per IT ACT, 2002

In India, the major regulation governing cybercrime is the Information Technology Act of 2000. Despite all this, primary goal was to acknowledge e-commerce in the country, it nowhere defined cybercriminals as such.[9] Section 43 of the Act might have been established to establish civil liability for " unpermitted access to anybody system or the local network that has been mentioned under subclause a and acting as an active accomplice to such an unlawful act (Subsection g) prior to its revision in 2008".[10] Phishing was covered by Section 66 (A), which is now considered unlawful. Section 66 B deals with obtaining any stolen work computer deceitfully. Identity theft is clearly defined in Section 66 C, and it is the only place in which it is defined. On the other side, Section 66 D was added to punish cheating through the use of computer resources. This clause appears to be comparable to the specialist committee's Section 419 A) suggestions described above. Penalties for privacy violations and cyberwarfare are among the other clauses included to the amendment. Sections 67 A and 67 B of the Act also give

[6] Defined under section 2(1) (ta) of the IT ACT, 2000 as "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.
[7] Added by Information Technology Amendment Act, 2008
[8] I.L.R. 2010 (3) Kerala.
[9] https://www.securitas.in/globalassets/india/files/about-us/news---related-documents/identity-theft-is-thelargest-contributor-to-fraud-in-india.pdf
[10] Un handbook on identity theft

aid to the vulnerable section of the society namely the women and children.[11] Furthermore, stricter legislation has been enacted to protect "sensitive personal data" in the control of middlemen and network operators (corporations), protecting data security and privacy. Only in extraordinary circumstances can such data be disclosed to a State or Central government department authorized for observation, continuous monitoring, or intercepting as mentioned and interpreted from the reading of section 69 of the said Act.[12]

The IT Rules of 2011 describe “sensitive personal data” as passwords, financial data, bodily, psychological, and mental medical problems, sexual preference, medical records and histories, and biometrics. In India, every 1 of every 4 people in India is has fallen prey of identity theft, according to a company's research findings, and such incidents have increased by 13% since 2011. [13]According to a proper research conducted from the team of analyst of Microsoft's reporting the safety index while using computer stated that, at least 20% of Indians have been victims of phishing attempts, with average losses of Rs. 7500. 41 When we consider that India's overall internet users account for about 19.9% of the population, the figures shown in this survey are rather significant.

The IT Act Amendment of 2008 has made one more addition to the act that is section 66-C to the IT Act of 2000, that in detail describes and punishes identity theft in the following ways: 'Whoever makes fraudulent or dishonest use of another person's electronic signature6, password, or any other unique identification feature. Any person found guilty shall be punished by putting him/her behind the bars for atleast a time that is not less than 3 years meanwhile there is no bar on charging fine that can range as high as upto one lakh rupees.'[14]

The conduct under this provision is cognizable, bailable, and needs to be tried by the court of first class magistrate. If one look at the Indian Penal code and read carefully the sections 24 and 25 , one would see that the terms dishonestly and fraudulently have been defined there. After carefully reading it with the newest addition in the IT Act , [15]it can be suggested that the identity theft is an intentional act on part of the perpetrator . This act can be anything and can include using the victim's electronic signature, password, or any other unique identification feature with the purpose of causing deliberate harm to the victim either by any of the following measure like downloading, extracting, or copying it. An electronic signature is a means of affixing an e-signature to an electronic record to authenticate it.

---

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

[12] 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)

[13] Ibid.

[14] 66 C

[15] 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).

Provision 66-D , which specifies in clear terms what exactly is the wrong and what shall be the kind of punishment that the person committing it would have to face , is another part of the aforementioned legislation that prohibits fraud via impersonating. This section of the IT Act can be defined as : 'Anyone cheats by personating by using any communication device or computer tool, and found guilty shall be punished by putting him/her behind the bars for atleast a time that is not less than 3 years meanwhile there is no bar on charging fine that can range as high as upto one lakh rupees.'[16]

The conduct is cognizable, bailable, and may be tried before the Magistrate of the First Class under this clause. A case was logged against nine people in the particular instance of the matter reported in the name of Samdeep Varghese v, State of Kerala, a case was made from the delegate of an organization where the organization primarily worked in the area of petrochemical industry and its trade and sale both internationally and nationwide and this individual was further accused of being privy to wrongs that have been mentioned under the IT ACT mainly the punishing clause that is section 66 (A – D) and other provisions relating to cheating from the Indian penal code

In this particular matter , 'www.jaypolychem.com' website was created by the alleged person Samdeep @ Sam who had been removed from the organisation, while acting in conspiracy with other participant of crimes. The content of this website was defamatory and malicious. The primary accused and the other co- accused sent emails from this website to the company's customers, their debtors, suppliers and banks via phone e-mail accounts with the goal of tarnishing the company's image. The first wrongdoer , together with other known and unknown individuals, conspired to defraud the firm and was a part of various acts of fraudulent activity , impersonating to be the company, and defamation, causing the company to lose several crores of rupees.[17]

The Different Formats of Identity Threat

On the one hand, digital mode has made conducting businesses and accessing public services such as paying electricity bills and completing income tax easier, but on the other hand, it has made our economic and legal data more vulnerable to crime. The following are the several types of identity theft.[18] The most frequent sort of identity theft is criminal identity fraud. In this case, the culprit illegally exploits the unwary victim's false identification to conduct any offense or trades it on the black market.

---

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

[17] 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-IJECSIJENS.pdf

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

Economic Identity theft happens when a perpetrator makes use of a victim's private details identity to commit deception or fraud involving bank balances, employment, as well as other financial matters with. [19] Offenders of identity clone and deception can utilize the data they acquire to disguise their actual self. They can demand and employ identifying devices to deceive investigators, or they can launder money through the victim's financial institution. They can also use stolen identities to get around identifying and terrorist prevention and detection.[20]

Synthetic identity fraud is a type of identity theft in which the offender utilizes fictitious material and hacked data to establish a new identity that is used for criminal purposes. To build a synthetic persona, multiple pieces of information are sometimes taken from multiple individuals.[21] Such a created identity, for example, can mainly be used to acquire a credit card, which can then be used to make transactions on the web or locally. Because their bank details is used, this type of identity theft can sometimes result in a victim's credit rating being lowered.

Medical identity theft happens when a thief utilizes a victim's healthcare care for their own gain. or health coverage benefits without permission, or when it is sold to cybercriminals.[22] In addition, the stolen identification is used to file and use bogus claims. As with other types of identity theft crimes, victims of this type of fraud may be subjected to a denial of service. The submission of a tax return with the use of a false identification and obtaining the rightful owner's rightful rebate received from tax was then classified as tax return identity fraud. The scammer may perpetrate financial crimes, result in slow or stolen returns, which is the third biggest theft of government funds after medical and government unemployment benefits. [23]Meanwhile While a stolen tax return may seem to be the deadliest scenario, a fraudster may also use a victim's phone identify to acquire employment, which is a far more dangerous conduct. When an identity thief uses another person's SSN to get employment. they must declare all of the money they make under that person's name.

The above discussion illustrates the numerous ways of online identity theft. There were two main types found. One would be the actual name for identity theft. The perpetrators in this case take their victims' personal information, which is then utilized fraudulently to obtain financial, medical, and other benefits by imitating the innocent people. The second one is the act of taking over an existing account

[19] 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).
[20] History of Computers, available at http://homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading03.html (last visited Oct 13, 2015).
[21] Vivek Tripathi, Cyber Laws India Cyberlawsindia.net, http://www.cyberlawsindia.net/index1.html (last visited Oct 13, 2015).
[22] India Risk Survey, 2014, (1 ed. 2014), http://www.ficci.com/Sedocument/20276/report-India-Risk-Survey2014.pdf (last visited Oct 13, 2015).
[23] India Risk Survey, 2014, (1 ed. 2014), http://www.ficci.com/Sedocument/20276/report-India-Risk-Survey2014.pdf (last visited Oct 13, 2015).

belonging to a victim in order to commit identity fraud.[24]This is typical case, intercepting victims' communications related to the financial activities and fraudulently transferring funds whose locations matched those of the con artists Criminal identity fraud, financial identity fraud, medical identity fraud, and synthetic identity theft are just a few of the most common. The issues concern not just financial damages, but also the health risks to which innocent people are exposed as a result of medical documents that have been tampered with.[25] Furthermore, victims may be tried and jailed for crimes they did not commit, or denied jobs and credit until their names have been cleared, which normally takes a long time and a lot of money.

The study also reveals that detecting some types of identity theft, uses information identity theft, can be difficult. This makes it very hard for law enforcement authorities to detect a scam, the cost of which will be carried in many cases by borrowers who have given fraudsters fake credit. Another thing worth mentioning is that youngsters are just as vulnerable to identity theft as adults. Because children's ssn are typically blank, fraudsters have a big target for exploiting the information.

As a result, children may be confronted with criminal histories that they are unaware of later in life. Essentially, online identity theft serves as a springboard for a variety of other sorts of cybercrime. As a result, it may include numerous stages, carried out at various times and locations and using various approaches. In the following section of this study paper, we'll look at some of the strategies utilized by online identity thieves.

Cases Relating to Identity Theft

Celebrities' personal identification information is considerably easy to obtain due to their celebrity and social engagement. It's because a lot is known about celebrities' lives, and much of the material is secured by a passcode that can be readily altered by anticipating the verification question's answer As a result, they are an obvious victim for Identity Theft. Michael Bloomberg, a well-known American businessman and owner, is at the top of this list.[26] Bloomberg LP Company is a subsidiary of Bloomberg LP. A thief exploited his details to remove a sum from his designated account via a web source , one more case where a cyber thief transferred $ 190,000 out of his own account using a forged check in Bloomberg's name. Likewise, a cybercriminal used golfer Tiger Woods' Social Security number, date and place of birth, and credit card details to make a $ 17,000 internet purchase. The famous actor Will Smith and singer Whitney Houston both had their identities stolen. [27]The Income Tax Portal, run by the Indian government, was targeted. A criminal from Hyderabad got entry to billionaire Anil Ambani's tax returns accounts, while the other one from Noida got

[24] Ibid.
[25] Supra note 9 .
[26] 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).
[27] Ibid.

entry to Sachin Tendulkar's , Mahendra Singh Dhoni and Shah Rukh Khan revenue tax records in two separate cases.

The RBI Phishing Fraud, the ICC World Cup 2011 swindle, and the password phishing fraudulent activity attacking Google email account subscribers are all examples of large-scale identity theft in India. In a very important case that shook the entire nation in the matter of NASSCOM v. Ajay Sood and Ors, the Delhi High Court found phishing on the internet to be an unlawful act for which penalties could be sued. This matter came to light in the early 2000s, a scenario in which there existed no proper guidelines that would prohibit phishing.

Impact of Identity Theft

Only those who are prey to this wrong can understand how this crime and its effect on the sufferers is no less than the traditional crime sufferers. It is proportional to the value of the identity thefts. has been utilized to conduct additional crimes. The wrongfully taken name using the information to create a social media footprint for the phone can be used to hurt the individual financially or smear someone. There is demonstrable monetary harm to the offender in the first scenario, but there is also an implied and incalculable loss to the perpetrator's image in both of the aforementioned cases.[28] To begin, where the victim's private details is utilized to commit financial crimes, the impersonator's default in repayment of bank loan and credit card dues, for example, is promptly reported by credit reporting agencies.

The true anguish for the victim occurs after the identity stolen has occurred, not because of initial crime (the cost of which is partially collected as damages in court), but also because the victim must have his or her reputation repaired and his or her record cleared from the credit agencies. This is a long and tedious step to follow, and the expense (with respect to the time and money, and the harassment that one has to survive during the entire procedure) is never taken into account by the relevant justice delivery system. As a result, this might be referred to as the victim's accounting method.[29]

In India, Credit Information Bureau (India) Ltd. (CIBIL) was the very first credit bureau in the nation. Equifax and Experian were among the bureaus that followed. These agencies keep track of a borrower's creditworthiness. When a lender files a fraudulent credit report on a borrower, or when a fraudster takes out loans or creates accounts in the names of the victims and fails to pay, the true holder of the identity may be rejected the appropriate credits. Also it is a very

---

[28] 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_theft s_and_online_frauds_in_the_era_of_internet_ijc_oct_2011.pdf (last visited Oct 13, 2015).

[29] 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)

difficult but even so if a person subjected to the wrong of identity theft goes on to prove that he in actuality is the real victim , he cannot recover damages. must contact the credit bureau himself to have his records changed. The victim receives no compensation for losses incurred as a result of incorrect credit agencies by lenders (such as banks) or delays in credit bureau repair. There really is no law in India that holds credit agencies liable or responsible for errors or omissions in an individual's credit report. The aforesaid technique can be used in the case of strictly financial offenses perpetrated by an thief, where the sufferer is able to show his or her is innocent without suffering significant societal consequences after being imprisoned. When stolen identity data is used to perform more serious crimes, such as creating a false victim's social media page with pornographic material or when they use the perpetrator's data to commit additional cybercrimes, the harm is far difficult and complicated to repair.

Problems in Indian Laws Relating to Identity Theft

Following its revision in 2008, the Information Technology Act of 2000 has gone a long way toward preventing an individual's private data from being exploited. Certain areas of the legal provisions on identity theft, however, require clarification or modifications. To begin with, the new Act's Section 66 C safeguards "unique identification feature," whose definition is not stated elsewhere in the Act.[30] The Information Technology Rules of 2011 define "sensitive personal information" as knowledge that middlemen must safeguard. However, unless the court understands "unique identification feature" to contain "sensitive personal information" whereas specifically authorised by legislation, this would be a push to equate "unique identification feature" with "sensitive personal information.."[31]

Second, despite the fact that the IT Act applies to anybody Whoever is responsible for identity theft using any computer resource in India is subject to Indian law questions remain unresolved. Third, the Act is insufficient in terms of the compensation paid to the victim. The compensation awarded is capped at 1 crore under Section 43 of the IT Act, and it is increased to 5 crore if the packet damage is committed by a legal person that can include all such types of entity that have a power to sue. The one has suffered loss , could lose more money than this, but that isn't taken into account. Furthermore, under Section 47 of the Act, when deciding a case claims under $5 million, the adjudicating officer must consider solely the victim's measurable loss when awarding compensation. As stated earlier in the article, the victim suffers a great deal of mental trauma and hardship as a result of the depending on the incident to which the personal identification material is subsequently applied. It requires a substantial

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

[31] 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).

investment of time and resources to restore a damaged image. image or rectify a credit record, which should be factored into compensation calculations.[32]

Fourth, under Section 66 C of the Act, the maximum fine for identity theft is I lakh. Identity fraud is a broad term that encompasses a variety of crimes of varying severity. An fraudster can steal property worth thousands of rupees from a single individual or millions of rupees from a huge community. A symbolic fine of not more than one lakh would've been issued in both circumstances. Furthermore, other provisions of the Indian Penal Code, which may be combined with the penalizing section of the said Act , but the problem remains that there is no specific amount that has to be charged can be tallied, limiting it in the hand of the judge to decide as per what he feels is appropriate.

Finally, laws are intended to fulfil a dual aim of crime prevention and deterrent. It is impossible to avoid identity theft by anticipating it. In the instance of this crime, a deterrent impact can be generated by investing a certain degree of malice aforethought or thought before committing it. This can be accomplished by applying harsher penalties and/or penalties. Identity theft is currently a cognizable, bailable, and result of an experimental manipulation offence under the IT Act. Compoundable crimes under Section 66 C are provided for in Section 77 A. Furthermore, a three-year prison sentence is insufficient and will not act as a deterrent.

Problems with Implementing the Identity Theft Laws

Despite the fact that cybercrime is becoming more common every year, India's number of convictions is shockingly low. According to 2013 data, just 7 of the suspects have been punished out of 3682 complaints. This could be owing to a poor infrastructure needed to enable the laws, or it could be due to inappropriate application of existing rules.[33]

Cyber thieves are increasingly employing new forms of encryption technologies and the development of technological advancements, which is difficult to interpret due to the authorities' scarce funds. This slows down the entire process, and in certain cases, the accused is released owing to a lack of evidence. Some legal decisions in the United States have allowed authorities the authority to ask a cybercriminal to decode digital evidence in exchange for reduced prison time, although this power has not been used frequently.

Finally, non-registration of cybercrime accusations by the authorities may be one of the causes for the low incidence of conviction or prosecution. This is an issue that should be investigated as well. These flaws can be addressed by the

[32] 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)

[33] 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).

government raising the number of openings for skilled law enforcement officers and giving out specific funds to more update the technology that is the most in market and that can help and contribute in the idea of coming face to face to a cybercriminal.[34]

Cyber Defamation

The phrase "cyber defamation" refers to the dissemination of false information about an individual in cyberspace with the intent to harm or defame that person's reputation. The offence of defamation is considered both a civil and a criminal offence in India, and the Indian justice system provides victims with legal recourse. If we consider the scenario today we would realize that this idea is a novel one , and the generic traditional defining clause of defamation would always mean the wrong done to a man's image and character in front of the rest of the world. This tarnishing could be inform of a written language or could be in form of a portrayal, anything and everything that a sane minded person would consider wrong. The term defamation when done on a digital platform is known as cyber defamation and would mean doing the exact thing as in the traditional form on a digital platform like using different online portals and other methods.

Cyber Negligence

However, there are grounds to doubt that requiring mandatory data security breach notification genuinely deters poor data security. The public, according to Schwartz and Janger, is unlikely to apply a large market sanction by rejecting enterprises with a history of poor data protection. In some circumstances, the breach will take place at a "backoffice" company that has no direct contact with customers (e.g. data processors, couriers or data brokers). Consumers are unlikely to know which "back office" service providers are utilized by particular retailers, making it harder for them to avoid those that have poor data protection. Customers will pay high switching costs with other sorts of firms, such as banks, and the market penalty for inadequate data security may be reduced.

Conclusion

The parliament should create mechanisms and rules to prosecute identity thieves. However, it is also critical to avoid data theft entirely by enacting tougher data protection laws. The network operators, essentially BPO and IT corporations that has details of the private information of people allacross the globe , are the main sources from which cyber thieves can obtain sensitive identity information. While India's data protection rules are not very robust at the moment, the proposed Personal Information Protection Bill is a move in the right direction toward enacting tighter data protection legislation.

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