ISSN: 2583-2751

BLIND FOLD LEGAL JOURNAL

VOLUME-2 ISSUE-4

{Mar. 2023 - May 2023}

E-Mail:- blindfoldjournal@gmail.com

Website: - www.blindfoldjournal.com

 ISSN: 2583-2751

COMPARITIVE STUDY ON IDENTITY THEFT: INDIA AND USA

Author: SENTHIL.V.P.

Abstract:

With the revolutionary change in technology and with globalisation digital adaptation prevailing in all fields Identity theft as a cybercrime has risen a lot in the past decade causing damage to consumers financially & to the economy as a whole. There are no special laws in India that cover the cybercrime component of identity theft, although they have recently been substantially incorporated into the IPC and IT Act. The provisions of Indian legislations only refer to this matter in respect to electronic records.

In USA there are slightly better laws to curb the issue of identity theft as a cybercrime. The paper critically analyses and compares the legislations of India and USA with relation to Identity theft as a cybercrime.

Keywords: Cybercrime, Electronic Record, Globalisation

Introduction

Identity theft is become a widespread problem. It is a very important place. It is said that identity theft is a crime of the modern era. The reality is that although certain effects of the information technology revolution have contributed to good progress, others—including identity theft—have grown to be a major worry.

Does identity theft pose worrisome concerns now? What harm does it do to society as a whole? How can it be handled? Questions pertaining to the problem need to be answered.

Research Objectives:

1. To determine the efficiency of Indian legislations on identity theft as a cyber rime in contemporary sense.
2. To assess the efficiency of US legislation on the same
3. To compare & critically analyse Indian & US legislation

Research Methodology

 ISSN: 2583-2751

Research undertaken is purely doctrinal and the data collected is primary source which includes statutes, legislations, case-Laws etc. Secondary source includes books, journals, articles etc.

Research Question

1. Whether IT act 2008 is effective in curbing Identity theft in India?
2. Whether U.S laws are efficient in tackling this offence compare to India?

What is Identity theft?

Definition

Identity theft is becoming a widespread problem. It is a very important place. It is said that identity theft is a crime of the modern era. The reality is that although certain effects of the information technology revolution have contributed to good progress, others—including identity theft—have grown to be a major worry.

Identity theft Statistics

According to expert research: Cyber Crime in India-2021 report from the National Crime Records Bureau, Bengaluru was responsible for 72% of the 1,685 identity theft instances that were reported across India's 19 major metropolises. Kanpur (119 instances) and Surat were the other cities where there were more identity theft cases reported (109).

Karnataka has also topped the list of states with the most identity thefts. 1,764 of the 4,071 identity theft instances reported nationwide in 2021 were from Karnataka. Bengaluru once again led the list among metropolitan cities for overall cybercrimes (including those reported under the IT Act, IPC, and special and municipal legislation) in 2021 with 6,423 incidents, followed by Hyderabad (3,303 cases), and Mumbai (2,883 cases). At the state level, there has been a shift in pattern. In the last three years, Telangana has seen an increase in cybercrime whereas Karnataka has seen a decrease. Cybercrime cases decreased in Karnataka from 12,020 in 2019 to 10,741 in 2020 and 8,136 in 2021. Telangana had a dramatic increase, from 2,691 cases in 2019 to 10,303 cases in 2021.[1]

[1] RAKESH PRAKASH , Bengaluru is identity-theft capital of India: NCRB ,TIMES OF INDIA (30.08.2022,06:57 AM), https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-is-identity-theft-capital-of-india-ncrb/articleshow/93865835.cms

 ISSN: 2583-2751

How does identity theft happen

The criminals use a variety of techniques to steal identities. But we'll talk about the top two ways:

- **Phishing**

Phishing is the practise of collecting personal data from recipients of shady emails. The email is presented to the recipient as coming from a reliable source or as something they specifically requested. a bank or the business where the receiver works, as an illustration.

- **Credit Card Skimming**

Victims of credit card skimming discover unauthorised financial transactions and charges on their accounts. The fact that all of this occurs while the victim is in possession of the credit card is astonishing.

It is a sort of credit card fraud in which thieves frequently utilise a tiny device to obtain credit card information, such as the cardholder's complete name, expiration date, and credit card number. A little device known as a "skimmer" is used to steal the information. When a person swipes their credit card on the skimmer, all of their personal information that was saved on the card's magnetic strip is acquired by the skimmer. These details are used by thieves to carry out fraudulent transactions and take the money. Once the information has been obtained, the thief can create a duplicate credit card and use it to complete several purchases. Theft from credit cards frequently goes unnoticed by the victims. The PIN for the ATM card can potentially be stolen by placing a covert camera.

Identity theft in contemporary society

In the current era of computerization, globalization, and the internet, our computers and other electronic devices collect a lot of data on each individual person and store it in archives hidden deep within the hard drive. Private information is stored in files like cache, internet history, and other temporary internet files, including login IDs and passwords, names, addresses, and even credit card numbers. In order to obtain sensitive and secret information, a hacker may use such sensitive information to gain unauthorized access to the data, share it with others, or even install dangerous software on a computer or other electronic device.

In our digital age, identity theft is a very important issue for everyone. It is a serious crime that is rapidly growing and causing economic harm to clients as well as prominent institutions, retailers, and the economic system across the nation. Electronic identity fraud has increased the variety of forms,

 ISSN: 2583-2751

making the situation more difficult. Such fraud may not only have a detrimental financial impact, but it may also severely hurt one's reputation, necessitate time to deal with rumours, and lead to exclusion from some services because the stolen name has been used inappropriately.

It is crucial to understand that computer networks can act as a base for theft or other harm committed online as well as a facilitator for identity theft, when the criminal seeks data online before doing the crime offline. Identity theft, the most recent and worst of a succession of horrifying white-collar crimes, has emerged as the crime of the century. At the end of the day, everyone is at risk because data fraud incidents are becoming more and more common. In emerging countries like India, incidents of identity theft and data fraud have rapidly escalated. Despite the Indian government's refusal to divulge statistics on the frequency of current identity theft cases, regular essays in newspaper columns can shed light on how risky and common these crimes are.

Identity theft legal analysis in India

Identity constitutes proof of the person's existence, but theft is the taking of anything without the owner's or the legitimate owner's permission. Identity theft happens when somebody steals over the identity of someone else without their permission or ownership. In plain English, identity theft occurs when a person copies or impersonates someone he is not. The Black Law Dictionary defines identity theft as "the unlawful taking and use of another person's identifying data for fraudulent purposes." Identity theft is a broad term that refers to a variety of crimes ranging from forgery to misrepresentation. Some of these crimes, such as ATM skimming and phishing, are regarded as conventional crimes, whereas others, such as the former.

The IPC and the IT Act, both define identity theft as a crime in India. Identity theft was made a felony after the IT Act of 2000 transformed the Indian Penal Code. These revised requirements are particularly focused on electronic records. The IPC, 1860 defines the electronic record similarly to how the IT Act, 2000 defines it, which is "data, record, or data created, picture, or the sound which is delivered or received by any electronic form."

Concerning the laws connected to identity theft, Sec 378 of the IPC, 1860's definition of "theft" Because it solely applies to transportable, physical goods and excludes cyberspace, it might not be applicable to identity theft. However, Sections 463, 464, 465, 469, and 474 of the Indian Penal Code, 1860[2], further, the laws for penalising forgery, and following the modification of the IPC, 1860,

[2] Indian Penal Code, § 463, 464, 465, 469, and 474, No. 45, Acts of Parliament, 1860 (India).

 ISSN: 2583-2751

identity theft was also brought within the purview of these provisions. However, the IPC, 1860 does not specifically mention "identity theft." Since identity theft involves impersonation-based cheating, it is equally punished under IPC sections 419 and 420.Identity theft is added to the Indian Penal Code, 1860, as an expanded form of forgery or deception, which skirts around the issue of making it illegal. The Information Technology Act of 2000 was amended in 2008, and as a result, the phrase "identity theft" was added. It took some time to realize that Sec 66C of the IT Act which covers the dishonest and immoral use of any identifiable attribute of any person, required offence-specific laws.

Another significant issue the judicial system has is actually putting these laws into practise. In India, there is not enough staff to handle the rising cybercrimes. Additionally, there is a dearth of knowledge about these significant cybercrimes, which contributes to the increase in identity theft instances. The National Cyber Security Regime (NCSP), published in 2013, emphasises the establishment of a national nodal agency and an appropriate, stringent certification policy, however it falls short in many respects. There is now just one certification policy available under the IT Act of 2000, the ISO027001 ISMS accreditation, which does not validate such certifications. NCSP does not have any intentions to adopt any further certification policies. Without offering a clear definition, the NCSP, 2013, also promotes adherence to open standards and public key infrastructure. Additionally, the policy expects to hire roughly 5 lakh people in the next five years, which is less than what will really happen. Overall, the National Cyber Security Policy of 2013 proven to be a flimsier and more distant notion than the core reality. Therefore, it may be concluded that these regulations appear to be enough for combating the crime of identity theft; yet, the rising frequency of reported cyber breakouts raises various concerns about the current legislation.

Laws protecting identity theft

- ATM skimming –

According to the court's ruling in Commissioner of Income Tax v/s. NCR Corporation Pvt Ltd.[3], ATMs are susceptible to cybercrime laws since any sort of computer is an essential part of an ATM machine and the physical function of cash dispensing or cash deposit is executed based on data processed by the related ATM unit's software. Therefore, under terms of the Information Technology Act of 2000, ATMs can be regarded as computers. There are extremely few laws that are compliant with and applicable to cybercrimes like ATM skimming in India since there are so few regulations

[3] Indian kanoon, https://indiankanoon.org/doc/190914707/ (10.11.22).

 ISSN: 2583-2751

that control cyber law there. ATM skimming is addressed in sec 43 and 66 of the IT Act of 2000. In addition to these two, more sections were added after the IT Act of 2008 was revised, including Sec 420 of the IPC and Sections 43A, 66C, and 66D.

Sec 43 of the IT Act of 2000 states that anyone who acquires, duplicates, presents a computer virus, harm, disrupts or causes delay, rejects accessibility, provides entry to any unauthorised individual in compliance with the act, or demands services that are used by any individual to an account of someone else is subject to civil liability. These Sec 43 requirements are included in Sec 63 to 74 of the IT Act of 2000. It should be noted that sections I and (j) cover more severe offences such as tinkering with the source code of a computer and modifying, destroying, or wiping any data stored in the computer resources. Sec 43, on the other hand, exclusively establishes the standards for third-party responsibility, not that of an information processor or controller.

The latest Personal Data Protection Bill, 2019, includes provisions for injury and the criteria by which these offenders can be held accountable. Without explicitly defining injury or damage, the Personal Data Protection Bill, 2019, defines "harm" as any situation that causes harm, whether physical or mental, loss, deformity, identity theft, loss of capital, or loss of property. The aforementioned description is more comprehensive of the important features of ATM skimming and serves to better clarify the criteria by which such offenders can be penalised. A corporate entity that possesses, interacts with, or manages any "sensitive private information" is neglectful in implementing or maintaining "justifiable security techniques and procedures," resulting in any negligent loss or gain, and is responsible to pay penalties to the damaged party. Sec 43A of the IT (Amendment) Act of 2008[4] makes this quite plain.

Such a description should provide a concise sketch of what might be considered a suitable practise and method rather than a thorough meaning. Appropriate security actions and procedures, as indicated in the explanation, may emerge by agreement, any existing legislation, or as specified by the CG in accordance with expert opinion as it deems fit. The CG has been given considerable authority and discretion in order to provide a proper interpretation to delicate private information and personal data that is still not classed under the Act. The Personal Data Protection Bill, 2019, attempts to clarify "personal information" and "sensitive personal information". while repealing Section 43A entirely. Furthermore, a body corporate's obligation has been split into the responsibilities of an information processor and an information fiduciary.

[4] Information Technology Act, § 43A, No. 21, Acts of Parliament, 2008 (India).

 ISSN: 2583-2751

The Personal Data Protection Bill of 2019 defines personal data as "traits, characteristics, attributes, or any other information about a natural person's identity, whether that information is online or offline." It also contains any information from which an assumption for profiling may be derived. When classifying sensitive private information, a broader perspective has been employed, including not just biometric data but also financial, health, sexuality, caste or tribe, intersex status, and sexual orientation. The Personal Data Protection Bill, 2019, also defines what private data and sensitive personal information are. According to the Personal Data Protection Bill, 2019, the authorities may categorise and penalise material as sensitive private data if exposing it would result in significant injury or violate a duty of secrecy. This phrase refers to the financial loss caused by the theft of private information through ATM skimming. The categorization of highly confidential data and the degree of severity of the penalty to be imposed, based on the loss caused by negligence and insufficient safeguarding by such data processors or data fiduciaries, both need improvement.

Every infringement of Sec 43 is subject to a 3 year prison sentence, a fine up to 5 lakh rupees, or both, as per Sec 66 of the IT Act, 2000. This includes ATM skimming, which is criminal culpability for other offences. Sections 66C and D, on the other hand, deal with punishments for identity theft and pretending to be another person in order to cheat by using a computer. These laws still need to define ATM skimming and skimming in general as separate offences.

In the case of Vidyawanti vs. SBI, the National Consumer Disputes Redressal Commission in New Delhi heard a revision petition.[5]. In this instance, many illegal transactions at the SBI ATM located at Karnal occurred through the complainant's account following a failed transaction at the ATM. The complainant sent a notice to the SBI of Patiala on the same day asking for a refund of the Rs. 40k that was improperly taken out of her account. The respondent didn't agree to the same. The petitioner then filed a suit. The court decided that it was clear from the evidence that was placed before it that 3rd party had compromised the ATM's resulting in illegal activities. Since the money was improperly taken from the complainant's account, the body corporate engaged in such banking operation made money off of it and was responsible for making up the loss to the harmed party. Because it would fall on the banks' responsibility to verify that the ATMs have not been tampered with and that they complied with the degree of safety, this ruling clearly defined the extent of the bank's liability for ATM tampering.

- Phishing

[5] Case Mine, https://www.casemine.com/judgement/in/590a0bc04a932663936d169b (10.11.22).

In National Association of Software and Service Companies v. Ajay Sood[6], the Indian judicial system defined "phishing." The Judiciary determined that "Phishing" is a class of online fraud. phishing includes, People who act as agents of online financial institutions and steal funds from consumers' e-banking wallets after deceiving them into providing their confidential financial data. Even while phishing is not a new issue, the assaults' quality is always rising, making it even more unexpected. The development of new distribution methods, such as instant messaging and social networks, poses novel dangers and makes it more challenging to identify phishing. The newest advancement in this area is vishing, commonly known as "voice phishing." Vishing assaults are carried out over the phone. Similarly, a contemporary approach known as "Smishing" is being employed to transmit phishing over SMS. So-called "Pharming" is the most recent iteration of phishing, in which the offender leads the target to a harmful website of their choosing. To make this happen, it converts an URL into a numeric IP that may be used to identify and drive users to the malicious website.

The IT Act of 2000 declares phishing to be unlawful in India since it involves the unauthorised obtaining of private data by masquerading a website as a trustworthy source. Sec 66, 66A, and 66D of the IT Act and Sec 420, 379, 468, and 471 of the IPC are a few statutes that apply to phishing. Anyone who sends an electronic communication with the intent to irritate, inconvenience, mislead, or confuse the addressee or recipient regarding the message's origin is in violation of the abolished clause (c) of Sec 66A of the IT Act. Phishing might have been added under clause (c) in this section because it is the act of misleading and tricking the intended recipient of an email, SMS, or other electronic forms. This clause, however, was eventually repealed in 2015 because it contravened the Indian Constitution's Article 19(2) guarantee of the freedom of speech and expression. However, cheating through impersonation is penalized by prison sentence as stated in Sec 66D of the IT Act, 2000, for a period duration that may extend to 3 years, as well as by a fine that may go up to 1 lakh rupees. Despite the fact that the term "phishing" is not used in this section, it is still included since it involves impersonating another person in order to defraud them of their information or money. Even though the number of phishing incidents is on the rise, no authority or process has been set up to address these issues. Reporting to the police station where the crime was perpetrated is the only way phishing victims may possibly receive relief.

Due to a lack of technology, the Indian police force is not well-equipped to solve these identity theft crimes. There must be a cyber-cell, or cyber-crime section in every police station or at least one in every district, for the police department to be able to take severe action. There are no specific

[6] National Association Of Software ... vs Ajay Sood And Ors, 119 (2005) DLT 596

 ISSN: 2583-2751

strategies to reduce the rising prevalence of identity fraud, not even in the National Cyber Security Policy of 2013.

Identity theft punishments

Anyone who uses another person's electronic signature, password, or other unique identification feature dishonestly or fraudulently is punishable by imprisonment of either kind for a term that may not exceed three years and by a fine that may not exceed Rupees one lakh, according to Section 66C of the IT Act, 2000.

Case References of identity theft

There are different cases through which we can understand Cyber Crime:

- CBI v. Arif Azim

Sony India Private Ltd. filed a suit against a non-resident Indians in this case. After making an online purchase, they were able to ship Sony items to their friends and relatives in India thanks to the website Sony Sambandh.

Arif Azim in Noida received a Sony Color Television and a cordless headphone as gifts from Barbara Campa, which is where it all began. After all the formalities were finished, the business sent the goods to Arif Azim. She made the payment using a credit card. Later, the credit card provider let the business know about the purchase. They stated that the actual cardholder had rejected the purchase and declared the transaction to be unlawful.

The business reported the incident to the Central Bureau of Investigation in accordance with IPC Sections 418, 419, and 420. Arif Azim was detained after an inquiry, at which point he admitted that while working at a contact centre, he had obtained access to a credit card number and had used it improperly.

The CBI found the headphones and television in this 2013 cybercrime conviction, which was a first for India. The accused pleaded guilt when the CBI presented evidence that supported its case. Arif was given a charge under Sections 418, 419, and 420 of the IPC, and the court released him on probation for a year since he was a young man of 24 years old and a first-time offender.[7]

---

[7] **CBI Vs Arif Azim, (2008) 105 DRJ 721: (2008) 150 DLT 769**

 ISSN: 2583-2751

- Nasscom vs. Ajay Sood & Others

This case has a historic ruling since it establishes the criminality of online "phishing," which can result in an injunction and the collection of damages. The National Association of Software and Service Companies (Nasscom), the leading software association in India, is the plaintiff in this lawsuit. The accused were the headhunting and recruiting placement firm that Nasscom employed. Defendants sent emails to other parties pretending to be Nasscom in order to get sensitive information they might use for headhunting. Therefore, phishing is an online scam in which a perpetrator poses as an organisation to steal clients' personal information, such as passwords or access codes, etc. Phishing is the practise of gathering personal information by impersonating a trustworthy entity and utilising it for one's own gain. Two hard discs from which the accused's emails to clients were transmitted were discovered by a committee the court designated to search the accused's property. The malicious emails were down loaded and used as proof. To avoid being identified and facing legal consequences, the accused adopted many false identities. Later, the accused came clean about their guilt, and both sides sought a settlement through negotiation. The defendants were awarded Rs. 1.6 million as compensation for the damages and infringement of their trademark rights caused by the accused. This case is crucial because it introduces the concept of "phishing" into the legal system and demonstrates that anybody who infringes intellectual property rights will be held accountable. This case restored confidence in the Indian judicial system's ability to defend intangible property rights.[8]

- Mphasis BPO Fraud, 2005

In this case, four consumers of Mphasis' client, The Citi Group, provided PIN information to four call center operators working in an outsourced facility in India owned by "Mphasis." These so-called employees lacked the qualifications necessary to get such PIN numbers. The employees conspired to open new accounts at Indian banks under false pretences. Utilizing the personal identification numbers and other account details they had obtained whilst working for Mphasis, they moved money over a 2-month period from the different financial accounts of The Citi Group clients to the newly opened bank accounts at Indian banks. United States-based bank had informed the Indian police of the scam by April 2005, and they had quickly located the offenders. Police apprehended the defendants as they attempted to withdraw money from the fake accounts. $230,000 of the $426,000 that was stolen might be retrieved. The sort of unauthorised access that was involved led the Court to

[8] Supra at 7

 ISSN: 2583-2751

conclude that Section 43(a) applied in this situation.[9]

- Syed Asifuddin and Ors. v/s. The State of Andhra Pradesh

In this case, Tata Indicom employees were imprisoned for changing the electronic 32-bit number, or ESN, that is encoded in cell phones that were expressly stolen with permission from Reliance Infocom. The Information Technology Act of 2000's Section 65 was deemed to have been violated by the Court as a result of such tampering with the source code.[10]

- Kumar v/s. Whiteley

The defendant in this case illegally got access to the Joint Academic Network (JANET), and he or she utilized that access to remove and add files as well as change credentials to bar authorized enterprise's users from using the system. Investigation revealed that Kumar, the accused, had "altered the computer database of broadband Internet user accounts" of the subscribers while attempting to enter onto the BSNL connection as the legitimate authorised user. Based on a report made by the Press Information Bureau, Chennai, which also discovered the unlawful abuse of broadband Internet, the CBI was forced to file a cybercrime case against Kumar and conduct investigations. Additionally, the lawsuit claimed that as a result of Kumar's wrongdoing, the subscribers had suffered a loss of Rs. 38,248. According to the Press Information Bureau, it was discovered that he had previously "hacked" websites from Bangalore, Chennai, and other places as well. The offender, Bangalore-based techie N G Arun Kumar, was sentenced by the Additional Chief Metropolitan Magistrate, Egmore, Chennai, to one year of hard labour in prison and a punishment of Rs. 5,000/- under Section 420 IPC (cheating) and Section 66 of IT Act (Computer Related Offence).

- Samdeep Vaghese v/s. State of Kerala

A complaint was filed against nine people by the representative of a company that traded and distributed petrochemicals both domestically and internationally. In addition to Sec 419 and 420 of the IPC, the complaint claimed violations of Sec 65, 66, 66A, 66C, and 66D of the IT Act, 2000. The company ran the www.jaypolychem.com website. However, the accused Samdeep Varghese set up another website, called "www.jayplychem.org," in the social platform in conjunction with another

[9] Molshree Totla, Pune Citibank Mphasis Call Center Fraud, Black n' White Journal (10.11.2022,9:00am), https://bnwjournal.com/2020/07/17/pune-citibank-mphasis-call-center-fraud/

[10] Syed Asifuddin And Ors. vs The State Of Andhra Pradesh, 2006 (1) ALD Cri 96

 ISSN: 2583-2751

accused, Preeti and Charanjeet Singh, who also happen to be Samdeep's sister and brother-in-law, respectively. On that website, damaging information and defamatory claims against the business and its directors were made available to the public. Sam's sister and brother-in-law, both accused and located in Cochin, conspired with other known and unidentified individuals to form the firm and commit fraud, impersonation, and other offences. Amardeep Singh and Rahul, two more defendants, frequently travelled to Delhi and Cochin. In order to harm the Company's reputation and those of its Directors, the 1st accused and others utilized phony electronic mail addresses pertaining to various clients, vendors, banks, etc. to send mails. The above-mentioned individuals' defamation campaign did significant harm to the Company's brand and reputation. As a result, the Company experienced losses from manufacturers, suppliers, and clients totalling many crores of Rupees and was unable to conduct business.[11]

Identity theft in USA

In USA FTC saw a rise in identity theft complaints in 2021. Identity theft occurs when a victim's personal information is used to create credit card or bank accounts, get a loan, or make transactions. According to the FTC, the number of consumer identity theft complaints in the U.S. increased by 3.3% from over 1.39 million in 2020 to little over 1.43 million. Government document fraud or benefits fraud continued to be the most prevalent type of identity theft in 2021, just as it was in 2020. This followed consumer alerts from the FTC and attempts by the agency's enforcement division to stop criminals from taking advantage of people's bewilderment and worry about the COVID-19 outbreak. Fraud involving official records or rewards garnered 396,012 complaints in 2021.

According to the FTC, credit card fraud, which was the most prevalent type of identity theft from 2017 through 2019, fell to second place in 2021 with 389,845 recorded occurrences. According to the FTC, out of the 603,591 identity theft occurrences recorded countrywide for the six-month period, credit card fraud generated 230,937 complaints in the first half of 2022, making it once again the most prevalent sort of identity theft reported in the nation.[12]

Applicable Identity Theft Laws In USA

[11] Indian Kanoon, https://indiankanoon.org/doc/1113321/ (10.11.2022)

[12] Jim Akin, Identity Theft Is on the Rise, Both in Incidents and Losses

, Experian (15.11.22,

10:00 am), https://www.experian.com/blogs/ask-experian/identity-theft-statistics/#s2

 ISSN: 2583-2751

Criminals who want to abuse personal information for illicit purposes value it highly. Criminals who stealthily gather personal information frequently have criminal motives, such as online impersonation, identity theft, or other illegal acts. Significant harm can result from identity theft. As a result, identity theft is prohibited by law in every US state as well as by the federal government. A thorough list of these statutes is available from the US National Conference of State Legislatures. Identity theft is prohibited under the following statutes in the US state of California:

- California Penal Code Section 368[13] — prohibits identity theft involving senior citizens and individuals with disabilities
- California Penal Code Section 530[14] — prohibits posing as someone else under a fake identity
- California Penal Code Section 530.5-530.8[15] — restricts the trafficking of personal data
- Penal Code Section 1202.4[16] — enables the court to issue a reparation order

To combat identity theft, the US federal government has established the following laws:

- Identity Theft and Assumption Deterrence Act— Amended Section 1028 of the 18 US Code to make identity theft illegal and a distinct offence against the victims. By authorising a maximum sentence of 15 years in jail, it also enhanced the penalties for fraud and identity theft.[17]
- Identity Theft Penalty Enhancement Act— prohibits aggravated identity theft, which is the use of another person's identity to perform serious crimes including stealing Social Security benefits and engaging in domestic terrorism.[18]

[13] California Legislative Information, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=368&lawCode=PEN (10.11.22)

[14] California Legislative Information, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=530.5.&lawCode=PEN (10.11.22)

[15] California Legislative Information, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=530.5.&lawCode=PEN (10.11.22)

[16] California Legislative Information, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=1202.4 (10.11.22)

[17] Federal Trade commission, https://www.ftc.gov/legal-library/browse/rules/identity-theft-assumption-deterrence-act-text (10.11.22)

[18] United States congress, https://www.congress.gov/bill/108th-congress/house-bill/1731 (10.11.22)

 ISSN: 2583-2751

- Identity Theft Enforcement and Restitution Act— Section 3663(b) of the 18 US Code was amended to make restitution-related matters clearer and to permit the courts to compensate victims for the time used to undo the harm.[19]
- Fair Debt Collection Practices Act— It is codified under Sections 1692 et seq. of the US Code and forbids debt collectors from using unfair or deceptive tactics. [20]
- Fair Credit Reporting Act— makes sure that credit reports collected by consumer reporting agencies, which are shared with other parties like financial institutions and other creditors, are accurate and private. Customers can dispute inaccurate account information and set up fraud alerts or security freezes to stop identity theft.[21]

  Criminals have employed a variety of techniques to commit identity theft, such as closely observing victims when they enter credit card or bank account details. Criminals may intercept a victim's electronic communications in order to obtain personal information, or they may send spam (unwanted emails) and demand personal data. Practically speaking, in order to increase security, IT professionals must understand how thieves get around security features on things like firewalls, network routers, and smart devices. Additionally, in order to prevent legal action from the government, IT professionals must abide by the relevant legislation. For instance, the US Federal Trade Commission (FTC) may file a lawsuit if a company breaches its promise to protect consumers' personal information.[22]

Privacy Related Laws of the US

The Fourth Amendment of the US Constitution, which forbids arbitrary government searches and seizures, grants citizens the right to privacy. In essence, the Fourth Amendment's primary goal is to safeguard individuals' right to privacy. The meaning of unreasonable searches and seizures has been influenced by court rulings. The Fourth Amendment is not violated, according to certain judges, by

[19] United States Congress, https://www.congress.gov/bill/110th-congress/house-bill/6060 , (10.11.22)

[20] Federal Trade Commission, https://www.ftc.gov/legal-library/browse/rules/fair-debt-collection-practices-act-text (10.11.22)

[21] Federal Trade Commission, https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act (10.11.22)

[22] Federal Trade Commission , https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (10.11.22)

 ISSN: 2583-2751

website monitoring technologies that expose email addresses or Internet Protocol (IP) addresses. The following federal privacy laws have been passed in the US:

- Driver's Privacy Protection Act— regulates the collection, use, and dissemination of personal data by US state departments of motor vehicles[23]
- Electronic Communications Privacy Act—safeguards electronic, spoken, and wired communications while they are being created, sent, and stored on computers. This federal law covers stored electronic information, telephone calls, and electronic messaging. [24]
- Family Educational Rights and Privacy Act— governs how public organisations, including prospective employers, publicly financed educational institutions, and foreign governments, can access educational records and information.[25]
- Privacy Act— establishes a code of fair information practises that regulates the gathering, handling, and sharing of personal data held in record-keeping systems by federal agencies.[26]
- Gramm-Leach-Bliley Act— Financial organisations are required to provide details on how they share and safeguard the private information of their customers.[27]
- Video Privacy Protection Act— provides clients with the option to choose not to have their personal information disclosed and the ability to take legal action if their rights are violated.[28]
- Federal Identity Theft and Assumption Deterrence Act— prohibits the creation, possession, or use of false, unauthorized, or other people's identities.[29]

Californians have an unalienable right to pursue and achieve privacy under the state's constitution. As a result, the law (including Penal Code Section 1546 and subsequent sections) requires that the government obtain a search warrant before accessing data on an electronic communication device. In California, the following laws protecting online privacy have been passed:

- The Anti-Phishing Act— phishing attacks are not allowed[30]

[23] Electronic Privacy Information Center, https://archive.epic.org/privacy/drivers/ (10.11.22)

[24] Bureau of Justice Assistance, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (10.11.22)

[25] U.S. Department of Education, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (10.11.22)

[26] US Department of Justice, https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition (10.11.22)

[27] Federal Deposit Insurance Corporation, https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-1-1.pdf (10.11.22)

[28] Electronic Privacy Information Center, https://epic.org/privacy/vppa (10.11.22)

[29] US Congress, https://www.congress.gov/bill/105th-congress/house-bill/3601

 ISSN: 2583-2751

- Consumer Protection Against Computer Spyware Act— prohibits the installation of malware on a person's computer[31]
- Education Code Sections 32261, 32265, 32270, 48900— Anti-cyberbullying legislation that forbids sexual harassment, harassment, violence motivated by hatred, and intimidation[32]
- Penal Code Sections 502, 647, 647.8, 786, and Civil Code Section 1708.85— Laws against internet exploitation forbidding retribution porn[33]

Consumers in the US State of California have the right to access, remove, and object to the processing of their personal data at any time under the Consumer Privacy Act (CCPA). It does not, however, include the right to correct inaccurate personal data, in contrast to the EU General Data Protection Regulation (GDPR)[34]. 24 Additionally, it mandates that websites include a privacy notice informing visitors of their ability to opt out. The right to privacy is not recognised specifically in the US Constitution. The California Constitution refers to the "inalienable right to privacy," which applies to both the state and private citizens. In reality, the courts have upheld this fundamental freedom. In the case of Hill v. National Collegiate Athletic Association, the Supreme Court specified the following methodology to assess whether a constitutional violation has occurred:[35]

- There must be a substantial violation of privacy interest
- a legally recognised right to privacy,
- an expectation of privacy that is reasonable.

Numerous class action lawsuits have been filed in relation to improper tracking technologies and internet privacy. In the Re DoubleClick Privacy case, for instance, customers claimed that DoubleClick—one of the biggest international suppliers of online advertising goods and services—

[30] California Business and Professions Code, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=33.&article= (10.11.22)

[31] California Business and Professions Code , https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=32.&lawCode=BPC (10.11.22)

[32] State of California Department of Justice, https://oag.ca.gov/cybersafety/children/cyberbullying (10.11.22)

[33] State of California Department of Justice, https://oag.ca.gov/sites/all/files/agweb/pdfs/ce/cyber-exploitation-law-enforcement-faqs.pdf (10.11.22)

[34] Intersoft Consulting, https://gdpr-info.eu/ (10.11.22)

[35] Supreme Court of California Resoruces, https://scocal.stanford.edu/opinion/hill-v-national-collegiate-athletic-assn-31368 (10.1122)

 ISSN: 2583-2751

was utilising illegal monitoring techniques to monitor their online activity. [36]The plaintiffs claimed that DoubleClick had injured them by violating their rights guaranteed by the state and federal constitutions. The class action was ultimately settled, and the defendant was required to pay a sizable sum for court costs and fees. Many jurisdictions in the United States have established laws and regulations that govern the notification processes for data breaches in order to promote consumer protection. However, offenders were successful in acquiring illegal access to the network servers of other firms. They have been successful in illegally obtaining personal data from network computers, which they then utilise for financial gain. Implementing data breach notification mechanisms is crucial as a result.

International conventions and laws relating to cyber crime

The Budapest Convention[37] on Cybercrime, commonly referred to as the Convention on Cybercrime or the Budapest Convention, is the first international convention aiming to combat Internet and computer crime by unifying national laws, enhancing investigative methods, and fostering international collaboration.

The only international agreement in this area that is legally enforceable is the Convention on Cybercrime. The document was developed by the Council of Europe with input from Canada, Japan, South Africa, and the United States, and it was made available for signing in Budapest in November 2001. It has been in effect since July 2004 and has taken on a global dimension as it provides nations with guidelines for the creation of national legislation against cybercrime, as more nations move toward ratification, and as it provides a framework for collaboration among the Parties to the Convention. The Convention requires that certain actions be made unlawful, such as unauthorised access to computer systems (also known as "hacking," "password-cracking," "key-logging," "exploiting software flaws," etc.), unauthorised data communications interception, data interference (such as malicious codes, viruses, trojan horses, etc.), and system interference (such as denial-of-

[36] United States District Court for the Southern District of New York, https://cyber.harvard.edu/is02/readings/doubleclick.html (10.11.22)

[37] UN ISPAC Conference on the evolving Challenge of Identity-related Crime, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3a1 (10.11.22)

 ISSN: 2583-2751

service attacks using botnets and other methods to prevent the legal use of computers). It calls for nations to enact a number of procedural laws to equip law enforcement and other criminal justice authorities with the tools they need to better investigate, prosecute, and judge cybercrimes. This should, among other things, give authorities the ability to act immediately in order to preserve electronic evidence, search for and seize computer data, or intercept communications, while also putting in place the necessary checks and balances to prevent abuse of these authorities and unnecessary violations of people's rights to privacy, freedom of expression, and other civil rights. The document concludes by outlining a number of steps for better global coordination in the fight against cybercrime.

The focus of the Convention is on criminal behaviour, not on particular methods or tools. Thus, there are no particular regulations regarding identity theft. The first and third steps of the ID theft process will be subject to criminal prosecution in States that fully implement the provisions of their substantive law: The question of whether stage two of the procedure, i.e., The use of identification information for any purpose should be made a separate criminal offence, as it is in the USA, for example, is still open in terms of substantive criminal law. The European Commission brought up this issue in Europe in a communication in May 2007. This will undoubtedly lead to more conversations and perhaps even acts. In addition to the restrictions imposed by substantive law, the Convention offers additional ways to support criminal justice measures against identity theft committed using computer systems. Any criminal offence involving a computer system is covered by the aforementioned procedural rules, which have a fairly broad scope. This implies that even if the behaviour isn't directly specified in the Convention, it can still be investigated if it's connected to ID theft and is considered a crime in the nation. The Convention's part on international cooperation is also very important because cybercrime is likely the most international of all crimes.

Nations that are committed to combating ID theft in connection to cybercrime should use all means possible to put the Convention on Cybercrime into practise. This will help in meeting many demands in terms of substantive law, procedural law, and international cooperation. However, it is still crucial to continue the discussion about whether or not it is also necessary to criminalise identity theft as a separate offence or to develop a unique international instrument on the criminalization of identity theft generally (that is not limited to the internet or computer systems), or whether or not making full use of the existing legal framework and emphasising prevention would be sufficient.

 ISSN: 2583-2751

Conclusion and suggestion

A person's privacy has been greatly violated by identity theft, which has had an impact on the victim's emotional and social well-being. Identity theft, however, has an effect beyond the person; it also poses a threat to businesses and organisations. From a legal perspective, Indian laws are weak when it comes to protecting identity theft, or the data of a person or business, leaving a lot of room for improvement in terms of laws, rules, and regulations pertaining to identity theft. The growing number of manipulative offenses, which have increased significantly in the past few years relative to the previous 2 decades, is facilitated by the lack of specific regulation. A robust system with an effective hierarchy of jurisdiction is required to guarantee sufficient execution of the current legislation and to equitably monitor the situation.

Additionally, it's important to prevent the abuse of authority and hire sufficient, kind people. Last but not least, the government has to educate the public on safe internet usage and measures to secure personal information. They also need to be informed about their legal rights and the appropriate channels for redress in the event of identity theft. People should also monitor their credit reports and any other places where personal data is utilised, and they should inquire as to why and how safe such data is being used in order to limit the harm and early discovery of identity theft.