Identity Theft: Extent and Applicability of Data Protection Laws

Abhishek Kushwaha & Aditi Palit[1]

Abstract

The nature of data protection laws in the light of identity theft and its analogue namely ATM skimming and Phishing pose obstacle before the existing cyber laws. Conventional laws have contributed to evolving number of personal data breaches. Virtual medium of interconnection among the computers called cyberspace not only provide with anonymity of users online but also works as a host to facilitate these high-end technical crimes. Drawbacks of personal data protection laws in Indian are evident in terms of legislations which are in turn only two Information Technology Act 2000 and Indian Penal Code 1860. The number of legislations which are inclusive of such techno forward crimes are alarming though attempts have been made in National Cyber Security Policy 2013 and Data Protection Bill 2019. ATM skimming is an act of altering the ATMs to make counterfeit of credit or debit cards whereas Phishing is an act of sending bogus emails luring customers to click. Uncertainty over accountability and liability of banks for acts of ATM skimming and Phishing gives fraudsters an upper hand. Contrasting the prospective of legislation, data protection system and initiative regarding personal data protection by financial institutes of United Kingdom to India indicate the glaring need of offence specific laws.

I. Introduction: Grey Area Of Cyberspace

> "As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace." - Newton Lee

Technology has fostered great advancements. One such advancement is the creation of arithmetical, logical and high-speed processing machines called Computers[2]. With the emerging trends of computers, the word 'cyber' appeared like a gate way to virtual reality. In order to integrate virtual reality to physical reality computers depend on optical or electrical impulses for establishing connectivity through cyberspace. This virtual medium which interconnects computers to other computerized devices through rapidly changing electronic combinations can be termed as cyberspace. According to National Cyber Security Policy 2013, the interactions between people, software and services which are supported by internet or worldwide distribution of networks and 'information and communication technology' (ICT) devices, such a complex environment is called cyberspace.[3]

Cyberspace is parallel to the oral and documentary mediums with no tangible attributes. The rise of cyber space as an alternative to its tangible counterparts can be subject to mala fide intentions when deflected from its intended use. Every person has a right to enjoy digital privacy and any disruptions caused due to interference by individual or computerized gadget are subject to cyber laws. According to Jay Dratler Jr. Cyber law addresses issues of online speech and business that arise because of the nature medium, including intellectual property rights, free speech, privacy, e – commerce, and safety, as well as questions of jurisdiction also termed as cyberspace law[4].

---

[1] Abhishek Kushwaha & Aditi Palit, Third Year B.A. LL.B. Amity Law School, Delhi.

[2] Information Technology Act, 2000, § 2.

[3] National Cyber Security Policy, 2013, Ministry of Electronic and Information Technology, (Jan, 13, 2020, 10:00 a.m), https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

[4] Henry Campbell Black, Black's Law Dictionary, pg. 443, (9 ed. Thomson Reuters: Minneapolis-St. Paul 2001).

Furthermore, he explained that Cyberspace law relates more to climbing the steep learning curve of the internet technological complexities than to changes in the accordance with accepted and well understood basic legal principles, albeit applied to new technology and new circumstances[5]. Hence to prevent infringement of right to digital privacy, legislators enacted Information Technology Act 2000 which had a sole objective of giving legal recognition and acceptance to electrical transactions carried in the virtual medium called cyberspace and for its legally sound use. According to the statement of object and reasons of Information Technology Act 2000 (IT Act 2000) the intention behind the enactment of IT act 2000 was to remove the hesitation surrounding the use computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form has many advantages such as it is cheaper, easier to, store retrieve and speeder to communicate. Such a reluctant behaviour is due to of lack of appropriate legal Framework[6]. Thus, IT Act 2000 would act as a trustful bond with humans and computers.

Technology has alleviated our perspective about boundaries of communications and transactions but as every cloud has a silver lining technology has paved a way for humans to embezzle the perks of it. The borderless space, anonymity of users' online, dynamic e-commerce and rapid inclusion of technology in businesses and organisations especially banking sectors is a stumbling block for the application of traditional cyber laws. Hence there is a glaring need for securing transactions online in order to restrain the criminal developers from having damaging consequences for such proliferate involvement of e-commerce.

Banks in order to have a competitive edge on being the most tech-savvy are expanding their services from "walk in office" to "available online" such services are exposing customer personal data making them prone to hacking, theft of personal data, phishing, spoofing for gaining unauthorized information to make illegal profits. Such acts may not appear to be illegal per se but can reverberate throughout the cyberspace causing immense danger and the customers are left to suffer the consequences. Initiatives towards the realm of securing banking assets include surveillance over both physical assets and intangible assets. More banks are prepared to counter the attacks, more criminals are equipping themselves with the latest technology to ensure that the banks always keep running -- to learn, to equip and to protect their assets.[7]

According to national crime record bureau [NCRB] reported ATM frauds and online banking frauds that were committed in all India in 2017 were about 1543 and 804 respectively. Whereas total reported cybercrime committed in India in 2017 are about 21796.[8]Not only ATM frauds, but ransom ware attacks like "WANNACRY" are also a threat to the digital world. The impact of WANNACRY in India may have been minimum extending its claws mainly in the state of west Bengal along with other metropolitan cities. But such a worldwide attack debunked the claims of the banking institutions and other e- commerce platforms for professing a safe and secure platform for their users. WANNACRY attack known as a Mega Cyber Attack has already became a global

[5] Henry Campbell Black, Black's Law Dictionary, pg. 443, (9 ed. Thomson Reuters: Minneapolis-St. Paul 2001).
[6] Statement Of Object And Reasons: Information Technology Bill 2000, Telecom Dispute Settlement And AppellantTribunal,(Jan,13,2020,10:00),http://www.tdsat.gov.in/admin/introduction/uploads/INFORMATION%20TECHNOLOGY%20ACT.pdf
[7] V. Rajendran, Banking on IT's Security, 89; The Journal of Indian Institute of Banking And Finance 13 (2018)
[8] Ministry of Home Affairs, Government of India, National Crime Record Bureau Report, National Crime Record Bureau (Jan, 13, 2020 10:25 am), http://ncrb.gov.in/StatPublications/CII/CII2017/pdfs/CII2017-Full.pdf.

phenomenon.[9] Other than malware intrusion, other offenders are also stepping up their game to knock down Indian laws on cyber security and data protection.

II. Data Protection Challenges:

a. Identity Theft

'Identity' is evidence of an individual's existence and 'theft' is possession without ownership or consent of the entitled person. Therefore, identity theft is when an individual possesses another person's existence without ownership. In layman's language identity is stolen when a person impersonates to be an individual who he is not. According to black's law dictionary identity theft is the unlawful taking and use of another person's identifying information for fraudulent purpose.[10] Identity theft is a very broad term and it extends to a considerable number of offences from misrepresentation to forgery, some are traditional crimes and some can be considered as newer versions of cyber-crimes like ATM skimming, phishing. All these offences are under the broad spectrum of identity theft.

In India identity theft is punishable under two legislations namely Indian Penal Code 1860 (IPC 1860) and Information Technology Act 2000. Identity theft as an offence was recognised after the Indian penal code was amended by the Information Technology Act 2000. The amended provisions in the Indian Penal Code 1860 specifically deal with offences related to the electronic record to be precise. Electronic record as defined in the IPC 1860 is identical under the IT act 2000 i.e. section 2(1)(t)[11]defines electronic record as data, record or data generated, image, sound which is sent or received through electronic form.[12]

Attention should be drawn to the provision which may include the offence of Identity theft. Theft[13] under IPC 1860 may not cover identity theft as it only extends to movable, tangible property and does not include cyberspace. Other provisions of the Indian Penal Code 1860 do not specifically mention identity theft but sections such as Section 463, 464, 465, 469, 474[14] these provisions penalised forgery and after the amendment identity theft is also included under the scope of these provisions. Under Section 419 and 420[15], identity theft is punishable as cheating specifically cheating by impersonation. Indian Penal Code 1860 beats around the bush to criminalize identity theft and adds it as an extended branch of forgery or cheating. The term 'identity theft' was added in 2008 amendment in the Information Technology Act 2000. It took few years to realise the need of offence specific laws, under section 66C[16] which penalises fraudulently or dishonestly making use of any unique identification feature of any person.
Implementation is another hurdle as there are no trained personnel to cope up with the constantly

[9]Ashok Koujalagi, Shweta Patil & Praveen Akkimaradi, The Wannacry Ransomware: A Mega Cyber Attack and Their Consequences on The Modern India, 6 International Journal of Management Information Technology And Engineering 4 (2018)
[10] Henry Campbell Black, Black's Law Dictionary, pg. 443, (9 ed. Thomson Reuters: Minneapolis-St. Paul 2001)
[11] Indian Penal Code, 1860, § 29.
[12] Information Technology Act, 2000, § 2.
[13] Indian Penal Code, 1860, § 378.
[14] Indian Penal Code, 1860, § 463, 464, 465, 469, 474.
[15] Indian Penal Code, 1860, § 419, 420.
[16] Information Technology Act, 2000, § 66 (c).

upgrading cybercrimes. Moreover, lack of awareness about such serious cyber-crimes feeds into the rising cases of identity theft every year. National security policy 2013 (NSP)[17] focuses on creating a nation nodal agency as well as proper and strict certification policy but still lacks in few areas. Currently under the Information Technology Act 2000 there is only one type of certification policy namely ISO27001 ISMS certification, which is not satisfactory and NSP does not include the notion to introduce more certification policies[18]. The NSP 2013 also encourages compliance with the open standards and public key infrastructure, without providing with a basic definition. Moreover, the policy targets at a human resource of creating 5 lakh personnel in next five year which falls short in reality[19]. Overall the national cyber security policy 2013 turned out to be superficial and far away from reality. From an over view the laws may seem to be sufficient to tackle the offence of identity theft but the growing number of reported cyber outbreaks question the existing legislations.

b. Identity Theft: Extended Branches

i) ATM Skimming

The idea of "cash anywhere, anytime" encouraged setting up of machines which allow easy withdrawal of cash by authorized account holders. Within a blink of an eye automated teller machines (ATMs) became primary and much needed facility provided by banks to their customers. ATM frauds are being conducted in various forms, from keypad overlays, hacking of the existing cameras, to installing cameras in the machine itself. Among all of these skimming is a much more advance form of financial fraud. Thus there is a requirement to approach it with a much more sophisticated and advanced security mechanism. Technophiles use skimming devices to commit theft. These new aged thieves can use hidden electronics devices like skimmer and false key pad overlay to copy all the personal information stored on a card and record the PIN number to access all that hard-earned cash from an individual's account[20]. Further this confidential information can be used to make counterfeit copy of cards inserted in such infected card insertion slots such an offence is known as ATM skimming[21]. Identity theft is only the beginning point as it branches out to other forms of offences this whole chain of events can incur financial losses. ATM skimming has not been specifically defined but ATM "Skimming" is an illegal activity that involves the installation of a device, usually undetectable by ATM users, that secretly records bank account data when the user inserts an ATM card into the machine. Criminals can then encode the stolen data onto a blank card and use it to steal money from the customer's bank account.[22]

ii) Are ATMs computers?

[17] The Ministry of Electronics and Information Technology, National Cyber Security Policy 2013, National Critical Information Infrastructure Protection Centre (Jan, 13, 2020, 10:00 am), https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf.
[18] Id.
[19] Id.
[20] Dr. Bharat Pancha, De-mystifying payment system challenges: Pragmatic Approach, 84(3) The Journal of Indian Institute of Banking & Finance 18-19, (2013).
[21] Id.
[22] Raymond W. Kelly, Crime Prevention Section Awareness Alert, Skimming at ATM Machines, Community Affairs Bureau and Police Department Of New York City, (Jan, 13, 2020, 10:00 am), http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/ATMskimmingtip.pdf

Aptness of legislation and accountability for such high-end sinister crime is also an angle which has to be considered while exploring the offence of ATM skimming. The only strand of legislation that to some extend can cope up with crimes related to ATM skimming is the Information Technology Act 2000 along with the information technology (amendment) act 2008.
Can ATMs be considered as computers or electronic devices to enable incorporation of offence relating to ATM within the preview of the IT act?

Thus, the question needs to be answered to ensure that the provisions of the only strand of legislation that is the IT act 2000 are applicable. Attention has to be drawn to the meaning of computers given under the IT act "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network[23], in simple words computers are expounded as electronic, magnetic, optical, high speed data processing layering the aspect of manipulation of electrical impulses to perform logical, arithmetical and memory functions moreover communication is established through inputs, outputs, processing , storage of such electrical impulses connected to other computers in a computer system or networks.

Emphasis should also to be given to the meaning of 'computer systems' interpreted as device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions[24] .Comparing the mechanism of ATMs they include input, output data as well consist of programmes to enable cash dispensation. All in all, the meaning and functioning of ATMs was analytically explained in the case of Diebold Systems Pvt Ltd Vs. Commissioner of Commercial Taxes[25] where the court stated that ATM has a data terminal with two input and four output devices. The ATM connects to and communicates with a host processor that is analogous to an Internet Service provider. Then the Machine is connected through the host processor through what is called a four-wire, point to point, dedicated telephone line. The ATM docs not have many parts, there is a card reader, which is what captures a person's account information that is stored on the magnetic strip located on the back of the ATM/debit card. This information is used by the host processor in routing the transaction to the appropriate bank. Then in has a 'Key pad', which is used by the cardholder to tell the machine what type of transaction is needed. It has an 'electric eye' that is used for cash dispensing mechanism. In addition to the eye, the ATM has a 'sensor' that is capable of evaluating the thickness of each of the bills being dispensed.[26]In a nutshell not only computers but all devices which are capable of inputs, outputs through electronic, magnetic impulses containing computer programs performing logical, arithmetical, communication control and other functions are computers, ATMs are not computer per se but are connected to other computers forming a computer network or system are covered under the Information Technology Act 2000.

[23] Information Technology Act, 2000, § 2.
[24] Id.
[25] Diebold Systems Pvt Ltd Vs. Commissioner of Commercial Taxes ILR, 2005 KAR 2210.
[26] Id.

Also, in the case of Commissioner Of Income Tax-III vs M/S NCR Corporation Pvt Ltd it was stated by the court that ATMs are under the jurisdiction of cyber penal laws as computer is integral part of ATM machine and on the basis of information processed by the computer in ATM machine only, the mechanical function of the dispensation of cash or deposit of cash is done[27]. Therefore, ATMs can be considered as computers within the preview of the information technology act 2000.

iii) Shortcomings of Existing Legislations.

With only handful of acts the existing reality of cyber law in India are evident. The working legislations are only scratching the surface instead of digging deep into the notion of security and accountability for such serious crimes. Provisions which deal with the offence of ATM skimming under the Information Technology Act 2000 are section 43, 66, whereas sections 43A, 66C, 66D added after the amendment in 2008 along with that other provisions such as section 420 of the Indian penal code. Section 43 of the Information Technology Act 2000 describes civil liability of a third party, where any person without the permission of the owner or the person in charge of access, downloads, copies, contamination of virus, damages, disruption or causing interruption, denial of access, gives access to any person who is unauthorised in accordance to the act, charges the services availed of by any person to the account of another[28]. The clauses under this section are accustomed to section 63 to 74. Whereas clauses (i) and (j) deal with more serious crimes related to tampering of computer source code, alteration, damage or destroying of any information residing in the computer resource[29]. But the section only provides with the liability of third party instead of data processor or data controller.

These added provisions may seem adequate from a bird's eye view but in contrast to the glaring number of skimming done in ATMs, they appear to be more open ended depending more on interpretation. words like '*injuriously by any means'*[30]and *'damage'*[31] are dependent on the interpretation of Court rather than expressively incorporating skimming done by third party, by physically altering the machines through insertion of foreign equipment causing financial losses punishable by penalty. Although attempt have been made in the recent Data protection bill 2019 to define the damage and the standard on which such fraudsters can be held liable. The Data protection bill 2019 does not define damage or injury but explains "harm"[32] which expressively includes bodily or mental injury, loss, distortion, theft of identity and financial losses or loss of property hence identifying the grade on which such offenders can be penalised which is more inclusive of some crucial aspects of ATM skimming[33].

Shortcomings on data protection and liability of the body corporate can be comprehensibly marked

[27]The High court of Karnataka, Commissioner of Income Tax-Iii vs M/S NCR Corporation Pvt Ltd, The High court of Karnataka (July 30, 2020, 10:00 A.M.), http://judgmenthck.kar.nic.in/judgmentsdsp/bitstream/123456789/333491/1/ITA242-11-16-06-2020.pdf
[28] Information Technology Act, 2000, § 43.
[29] Information Technology Act, 2000, [Amendment 2008], § 43.
[30] Information Technology Act, 2000, § 43.
[31] Id.
[32]Ministry of Electronic and Information Technology, Data Protection Bill 2019, MEITY (Jan, 13, 2020, 10:00 am) https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.
[33] Id.

in section 43A[34] where a body corporate possessing, dealing or handling any 'sensitive personal data' is negligent in implementing or maintaining 'reasonable security practices and procedure' causing wrongful loss or wrongful gain shall be liable to pay compensation to the person so affected[35]. Reasonable security practices and procedure as mentioned in the explanation may arise by way of agreement, any law in force or as prescribed by the central government in consonance to expert advice[36], such explanation only provides with a brief outline of what can constitute as reasonable practice and procedure rather than providing a comprehensive meaning to it.

Secondly a wide power and discretion have been given to the central government on providing with an appropriate meaning to sensitive personal data as well as personal data which have not been yet classified in the Act. But an effort has been made in the Data protection bill 2019 to give meaning to 'personal data' and 'sensitive personal data' while omitting section 43A completely and fragmenting the liability of body corporate into liability of data processor and data fiduciary[37]. Personal data includes trait, characteristics, attribute or any other information of a natural person about the identity of such person whether online or offline also may include any data or information from which an inference can be drawn for the purpose of profiling[38]. A more of a contemporary approach have been taken while defining sensitive personal data, which not only include biometric, financial, health, sex life, caste or tribe, but also include transgender status, intersex status and sexual orientation[39]. With reference to what can be considered as personal data or sensitive personal data the bill also includes an explanation, that if disclosure of such data may cause significant harm or if there is an expectation of confidentiality such can be classified and sanctioned as sensitive personal data by the authority under the bill[40]. Such a definition incorporates the loss of personal information through skimming of ATM cards and the subsequent financial loss as sensitive personal data. Still a little wiggle room is left in terms of the categorisation of sensitive data and penalty to be imposed according to the seriousness of the loss occurred due to the negligence and disinvestment of adequate security by such data processor or data fiduciary. Criminal liability for ATM skimming is covered in relation to other offences under section 66, explains that any offence covered under section 43[41] is punishable with imprisonment for a term of 3 years or with fine which may extend to five lakh rupees or both[42]. Whereas section 66C and 66D[43] deals with punishment for identity theft and cheating by impersonation by using computer resource. The available provisions are still are not inclusive of ATM skimming or skimming in general as a specific offence.

iv) Liability of banks or third party?

Confusion is there with regards to the accountability and liability of the banks in terms of frauds committed by the third party especially for ATM skimming. Followed by the extent of customers

[34]Information Technology Act, 2000, § 43.
[35]Id.
[36]Id.
[37] Supra, 32
[38] Id.
[39] Id.
[40] Id.
[41] Information Technology, Act, 2000, § 43.
[42] Information Technology, Act, 2000, § 66.
[43] Information Technology, 2000, § 66D, § 66C.

personal liability and denial by banks is giving the offenders an upper hand in such techno forward crime. In 2015 in the case of Vidyawanti vs. State Bank of India[44] a revision petition was made by the petitioner to the National Consumer Disputes Redressal Commission, New Delhi. In this case, after a failed transaction at the ATM of State Bank of India installed at Nehru Place, Karnal, unauthorized transactions took place at the ATM through the account of the complainant. On the same day, complainant wrote a letter to State Bank of Patiala seeking refund of Rs. 40,000 wrongfully withdrawn from her account but the respondents/opposite parties failed to oblige. This led to filing of the consumer complaint. It was held that from the evidences it is clear that a third party has manipulated with the ATM machine which has resulted in unauthorized transactions. As the money has been wrongly withdrawn from the account of the complainant, the body corporate who are in banking business and earning profit out of it are liable to make good her loss. This case clearly defined the scope of the bank's liability in terms of manipulated ATMs as the burden of responsibility would be on the banks to make sure the ATM machines are not altered and ensuring compliance of the standard of security[45].

The concept of 'no fault liability' of the banks with respect to ATM related frauds especially skimming was considered in the notification of (reserve bank of India) RBI in July 6, 2017. The RBI broke down the liability of the customer into following segments:

a. First is the 'Zero liability', a customer is entitled zero causality in case where the transaction occurred due to negligence of the banks whereas in case where the fraud is occurred neither due to the fault of banks nor the customer but lies elsewhere in the system then, if the customer notifies the bank within 3 working days then the customer would be entitled to zero casualty[46].
b. Secondly the concept of limited liability of customers in cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials. In that case the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reported unauthorised transaction shall be borne by the bank[47].
c. In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay on the part of the customer in notifying the bank about the unauthorised transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in the notification, whichever is lower.[48]

Therefore, liability lies with multiple entities in a single unauthorized transaction but the most affected are the consumers. Even in the concept of zero liability, limited liability or when there is a delay in the redressal process the initial loss has to be borne by the customers.

v) Phishing

Phishing is not a contemporary issue in the cyberspace but its variants have been evolving through time. It is one of the most common types of cyber-attack on an individual's right of security. The

[44] Vidyawanti v. State Bank of India Iii, CPJ 2015 NC 245.
[45] Id.
[46] Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking, Reserve Bank of India (Jan, 13, 2020, 11:43 am), Rbi/2017-18/15 Dbr. No. Leg.Bc.78/09.07.005/2017-18.
[47] Id.
[48] Id.

general definition of phishing as per the oxford dictionary is that it is a fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information such as passwords and credit card numbers[49]. Moreover Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit or debit card information from users[50].In layman language it is a activity of tricking people into giving their financial identity like bank account numbers, pan card numbers, account passwords etc. over the Internet or by email or by other means, and then using this sensitive information to dupe them of money.

Indian judiciary system has interpreted phishing in the case of National Association of Software and Service Companies v. Ajay Sood. The court held that, Phishing is a form of internet fraud. In a case of phishing, a person pretending to be a legitimate association such as a bank or an insurance company in order to extract personal data from a user such as access codes, passwords, etc. which are then used to his own advantage, misrepresents on the identity of the legitimate party. Typically, phishing scams involve persons who pretend to represent online banks and siphon cash from e banking accounts after conning consumers into handing over confidential banking details.[51]

There are upgraded variants or techniques that are employed by phishers which can essentially be grouped under these headings. First and foremost is the one involving use of spam email, websites and pop up window or fake banners. The second is where the advertising bears false corporate identification that are addressed to a large number of people this does not require specific identification of victims in advance rather it requires a response from the victim to accrue information causing identity theft[52]. These include Nigerian lottery emails and home/reshipping schemes[53]. The recent example is of Paytm KYC (Know Your Customer) registration through SMS for using the payment gateway.

Though phishing is not a new threat but the constant upgradation of the attack, is making it less and less predictable. The introduction of new channels of distribution, like instant messaging and social networks are posing new threats and detection of phishing is more difficult. Vishing or also known as voice phishing is a much recent development in the field. This attack is perpetrated through a phone call. Likewise, Smishing is a new technique that is used to phish through SMS. Pharming is the newest method of phishing where the attacker redirects the victim to a malicious site of their choice. This is done through converting an alphabetical URL into a numerical IP address so that it can locate and direct the visitors to the malicious website[54].

vi) Available legislations

[49] Oxford University Press, Oxford Advanced Learner's Dictionary, Department of the University of Oxford, (July 30, 2020, 10:00 A.M.), https://www.oxfordlearnersdictionaries.com/definition/american_english/phishing
[50]Jyoti Chhikara, Ritu Dahiya, Phishing & Anti-Phishing Techniques: Case Study, 13(5) International Journal of Advanced Research in Computer Science and Software Engineering 5 (2013).
[51] National Association of Software and Service Companies v. Ajay Sood, 2005 119 DLT 596.
[52] Supra, 50
[53] Australian competition and consumer commission, Nigerian Scams, SCAMWATCH, (Jan, 13, 2020, 10:00 am) https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams
[54] Ezer Osei Yeboah-Boateng, Priscilla Mateko Amanor, Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices, 5(4) Journal of Emerging Trends in Computing and Information Sciences, (2014).

In India, under the Information Technology Act, 2000 phishing is punishable. Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity[55]. Provisions which are applicable on phishing are Sections 66, 66A and 66D of Information Technology Act 2000 and Section 420, 379, 468 and 471 of India Penal Code, 1860[56]. The repealed clause (c) of section 66A of the IT Act which states that an act is punishable if *any person, through computer resource, communication device, any* electronic mail or electronic mail sends a message for the purpose of causing annoyance, inconvenience, to deceive or to mislead the addressee or recipient about the origin of such messages[57].In this section the act of phishing could have been included under clause (c) as phishing is an act of deceiving and misleading but this section was later struck down in the year 2015 being against the freedom of speech and expression under the Article 19(2) of the Constitution of India.[58]However, *Section* 66D penalises cheating by impersonation by means for any communication device or computer resource with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees[59].Though this section does not mention the word phishing but is still inclusive of Phishing and its extended forms as in phishing there is impersonation for the purpose of cheating or duping people to extract data.

The act of phishing though is an act of fraud from a third party but the act is done through online means. Thus, banks have the responsibility to make the users aware of these kinds of frauds. That said, there is no legal duty of the banks to do so but rather a moral duty. The only liability is of the third party i.e. the party which has committed the crime of phishing.

While phishing cases are rising in number but there is no mechanism or authority in place to take cognizance of these matters. The only possible way for the victims of phishing to find remedy is to report at the police station where the crime is committed. Due to lack of technology, the Indian police department is not at all equipped to solve these identity theft related crimes. For the police department, to be able to take stern actions it is required to have a cyber cell at each district if not at every police station[60]. Even in the recent National Cyber Security Policy 2013 there are mere suggestions but no actual method has been formulated to reduce the increasing number of identity frauds[61].

vii) Comparison to other countries

When compared to the US they have appropriate system for reporting of phishing crimes. Jeffrey Brett Goodin became the first convicted cybercriminal by a jury in 2007 under the CAN- SPAM Act, 2003 for sending thousands of e-mails to online users which prompted customers to submit personal credit card information[62]. The CAN-SPAM Act is an act that is the direct response of the alarming number of complaints over spam e-mails and is also the first American cyber law which establishes the national standards for sending commercial e-mails. These standards keep these

[55]Singh, Netra, Online banking Fraud Using Phishing, 12 Journal of Internet Banking and Commerce 1-27 (2007).
[56] India Penal Code, 1860, § 420, 379, 468, 471.
[57] Information Technology Act, 2000, § 66A (c).
[58] Shreya Singhal v. Union of India, 2010 12 S.C.C. 73.
[59] Information Technology Act, 2000, § 66D.
[60] Supra, 55
[61] Supra, 17.
[62]Jeffrey Brett Goodin v. The United States of America, 28 U.S.C 2255 (2010).

phishing activities in check[63]. In India there is no body or reporting system for specific offences like phishing. There is a dire need for these types of standards in India. The Information Technology Act 2000 has provisions that include phishing but there are no offence specific provisions.

In the United States of America, the Electronic Communication Privacy Act 1986 was the first act to regulate the internet related issues, prohibiting unauthorized intentional access to facility or network and the interception of data. This act had both civil as well as criminal penalties[64].

In England, the Anti-Fraud Act as passed in the year 2006 and in Wales and Northern Ireland by the name Fraud Act, 2006[65]. This Act banned the usage of phishing kits for creating and sending e-mails in millions. This Act punishes frauds by the means of false representation, fraud by failing to disclose information and fraud by abusing one's position. This act was the first to punish the act of phishing[66].

III. Comparison: Cyber Policies of United Kingdom

A walk towards liberalisation paved way for cyber offences to dig its roots deep into the territorial boundaries of India. Comparing and contrasting the policies of countries such as United Kingdom which are having elevated defence mechanisms leaves us with the shortcomings of Indian laws. First stage of comparison can be made on the bases of legislative prospective. To meet the international standards India was reluctant to offer high level of security in the realm of cyberspace. Legislations related to cyberspace began with the enactment of Information Technology Act 2000 with a view to frame a backbone of cyber security in India which ended up with loopholes and incomplete interpretations. To underpin Information Technology Act 2000, in 2004 a statutory body under the Ministry of Electronic and Information well known as the Indian computer emergency response team [CERT-IN] was formed[67]. The objective of CERT-IN was to forecast, alert and take emergency measures for handling cyber security incidents. It was also responsible for providing with annual statistics on cyberattacks[68]. Shortly, an amendment was made in 2008 to broaden the penalising aspect of the Information Technology act 2000.

The amendment was done to ensure a more defined role to CERT-IN and to include identity theft and data protection at an individual level only to settle for an overview of theoretically adequate laws. Policies such as National Encryption Policy[69] and National cyber security policy were only

[63]Federal Trade Commission, CAM-SPAM Act 2003, Federal Trade Commission Protecting Americas Consumer, (Jan, 13, 2020, 10:00 am), https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf

[64]United States Department of Justice**,** Electronic Communications Privacy Act of 1986 (ECPA), Justice Information Sharing, (Jan, 13, 2020, 5:00 pm), https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

[65]Government of United Kingdom, Fraud Act 2006, the Crown Prosecution Service, (Jan, 13, 2020, 5:00 pm), https://www.cps.gov.uk/legal-guidance/fraud-act-2006

[66] Id.

[67]Ministry of Electronics and Information Technology, Government of India, Welcome To CERT-IN, Indian Computer Emergency Response Team, (Jan, 13, 2020, 5:00 pm), https://www.cert-in.org.in/

[68]Ministry of Electronic and Information Technology, government of India, ICERT, Indian Computer Emergency Response Team (Jan, 13, 2020, 5:00 pm), https://meity.gov.in/content/icert

[69] Ministry of Electronic and Information Technology, Government of India, National Encryption Policy, Ministry of Electronic And Information Technology, (Jan, 13, 2020, 5:00 pm), https://meity.gov.in/writereaddata/files/national-encryption-policy-govt_0.pdf

like a statement of first principles. The National cyber security policy 2013 was introduced with a strategy for implementation of integrated approach to guide the policy actions of various institutions that would result in establishment of national and sectorial CERT-IN and CERT respectively as well as formation of national information infrastructure protection centre [NCIIPC][70]. In United Kingdom the case of *Regina v Gold and Schifreen*[71]in which the court of appeal coined that the laws in the country were not adequate enough and incapable to deal with cybercrime thus UK was the first country to enact a legislation in the realm of cybercrime, the computer misuse act 1990 penalised only 3 offences namely unauthorized access to computer material[72], access with intent to facilitate an offence[73], and unauthorised modification of computer material[74]. In 2006, the act was amended by the Police and Justice Act 2006 which increased punishment for the already incorporated 3 offences and added another offence of supplying or obtaining article for the offences mentioned section 1, 2, 3[75]. It is crystal clear that UK realised the need for protecting cyberspace long before India drafted its first legislation to tackle cybercrime and took years to rectify the shortcomings. Computer misuse act 1990 even though a primary legislation but to some extent is on point to criminate offences of skimming and identity theft[76].

Second stage of comparison could be drawn out in terms of Data protection. Apparatus for Data protection in India can be widely concluded through the national cyber security policy 2013 where data protection was made a priority but among the prescribed ways only few were operational and most of the steps mentioned in the policy are vague with whole and sole responsibility on the government to implement the policy. Authority established under section 70A of the IT act 2000[77] namely National critical information infrastructure protection [NCIIPC] focuses on establishing system of critical information infrastructure [CII] to rank the sectors for protection on the bases of "criticality"[78]. Under the common law applicable in UK where there is a 'sufficient relationship of proximity' duty of care is owned to another party whose act of carelessness harms the victim.[79] Individual privacy is considered as a basic human right the person having control over such sensitive information has an established relation to make him liable towards the owner of such information. Considering privacy as a right, Data Protection Act 1998 was enacted to comply with the EU regulations for privacy to ensure data protection by data controllers as well as penalization of unauthorised access[80]. National cyber security strategy 2016 specifically in based on the principles of defend, deter, develop. Moreover, the established National Cyber Security Centre which combined parent body GCHQ and other statutory bodies CPNI, CERT-UK, CCA,

[70] Supra, 17.
[71] Regina v Gold and Schifreen, 1116 CACD, QB (1987).
[72] Computer Misuse Act, 1990, § 1.
[73] Computer Misuse Act, 1990, § 2.
[74] Computer Misuse Act, 1990, § 3.
[75] Id.
[76] Government of United Kingdom, Computer Misuse Act 1990, legislations.gov.uk, (Jan, 13, 2020, 5:00 pm), https://www.legislation.gov.uk/ukpga/1990/18/contents
[77] Information Technology Act, 2000, § 70A.
[78] Ministry of Electronic and Information Technology, Guidelines for critical information infrastructure, National Critical Information Infrastructure Protection Centre, (Jan, 13, 2020, 10:00 am), https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf
[79] Caparo Industries Plc v. Dickman, 2 Ac 605 (1990).
[80] Government of United Kingdom, Data Protection Act 1998, legislations.gov.uk, (Jan, 13, 2020, 5:00 pm), https://www.legislation.gov.uk/ukpga/1998/29/contents

CESG[81].Still Indian laws lack in unifications, there is no centralised authority to counter the data theft. On comparing UK laws to the Indian laws, later are vague, more focused on cyber terrorism and protecting governmental database rather than individual data, whereas the National Cyber Security Strategy 2016 balances between three components government, business and individual[82]. While contrasting the Indians statutes with United Kingdom, former have a more defensive approach than an offensive approach.

Third stage of comparison can be made on the basis of individual data protection and related offences. In India section 43, 43A, 66, 66C, 66D, 72, 72A of the IT act deal with identity theft, ATM skimming and phishing. The liability of such offences as per reserve bank of India notification rule 3 mandates banks to invest in cyber crises management plan to combat early threats and such unusual cyber inferences has to be reported to RBI[83]. Hence such offences are governed by notification of RBI. Whereas in UK there is no specific authority but the Financial Conduct Authority covers the area of system controls over financial fraud[84]. Moreover, General Data Protection Regulation 2018 [GDPR] puts a mandatory obligation on the organisations to notify the individuals about data breaches which are likely to occur and such breach should also to be reported by the organisation to information commissioner's office within 72 hours[85]. Overall responsibility is on the organisation to carry out work according to GDPR. Under the anti-fraud act 2006 of England, wales and norther Ireland, phishing kits are banned for sending and creating bogus emails. Thus, Indian laws are on a back foot when it comes to individual data breaches leaving room for improvement in policies made in favour of identity theft[86].

IV. Conclusion

Thus, Indian laws are on a back foot when it comes to protection of an individual's data, leaving a lot of room for improvement in laws as well as policies made in favour of identity theft. The laxity in specific laws, acts as a host for such manipulative offences which have become more and more common as compared to the last two decades. Indian cyber law lack in core implementation and requisite expertise to curb identity theft, ATM skimming and phishing. To ensure adequate implementation of the existing laws, there arises a need to establish proper system with efficient hierarchy of jurisdiction. Overlapping of power should be curbed, and adequate humane personnel should be employed. Advanced laws of different countries like United Kingdom could work as a frame for improvement in existing laws along with the national cyber security policy 2013 which

[81] Government of United Kingdom, National Cyber Security Strategy 2016, HM government, (Jan, 13, 2020, 11:43 am),https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[82] Id.

[83] Reserve Bank of India, Basic Cyber Security Framework for Primary (Urban) Cooperative Banks, Reserve Bank of India notifications, (Jan, 13, 2020, 12:15pm) https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT636E1566334F9A4F998C838D5AC6173A96.PDF

[84]Government of United Kingdom, Chapter 3: Sysc 3.2 Areas Covered by Systems And Controls Rule, GUIDANCE Sysc 3.2.6, Financial Conduct Authority Handbook (Jan, 13, 2020, 1:00 pm) https://www.handbook.fca.org.uk/handbook/SYSC/3/2.html

[85] Government of United Kingdom, General Data Protection Regulation 2018 [GDPR], Information Commissioner's Office, (Jan, 13, 2020, 1:00 pm), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

[86] Government of United Kingdom, Fraud Act 2006, the Crown Prosecution Service, (Jan, 13, 2020, 5:00 pm), https://www.cps.gov.uk/legal-guidance/fraud-act-2006.

involve adequate framework for laws but lacks implementation. India lies at the base of well-developed cyber laws; however, attempts such as Data Protection Bill, 2019 may contribute in the quest to achieve security of personal data of individuals.