LAW MANTRA THINK BEYOND OTHERS
(International Monthly Journal, I.S.S.N 2321 6417)
Journal.lawmantra.co.in www.lawmantra.co.in

FINANCIAL VICTIMIZATION THROUGH CYBER TOOLS AND PARADIGM SHIFT IN CRIMINAL LAW DEFINITIONS: A COMPARATIVE SKETCH

BY ASST.PROF. GAURAV KATARIA(Ph.D.)*

Introduction:

The crime has never been that leisurely for criminals. Neither a robber needed gun to rob a bank nor does a burglar need implements for house breaking. The computer's role is analogous to commit any crime against property or against body. The cyber means are increasingly used by organized criminal groups to target credit cards, bank account and other financial instruments to commit crime against property. Online theft of property is considered to be third amongst economic crimes prevalent in India according to Global Economic Crime Survey 2011, conducted by Price House Water House Cooper[1], which reveals the propensity of such crimes in India. In such instances of cyber crime, the computer is used as a tool. The cyber criminals employ to commit a crime involving computer technology but not directed at a computer victim. The law should be dealt with target cyber crime and tool cyber crime differently. The target crimes are required adoption of the new laws. The conduct involved and the harm inflicted by such target cyber crimes is not encompassed by traditional criminal law. In the tool crime the computer plays a lesser but still far from insignificant role in the criminal activities. Target cyber crime is primarily concerned with harm to a computer or computer system while tool cybercrime are concerned with the other harms which the criminals can inflict by exploiting computer technology. More precisely, they are concerned with the other harms defined in the Indian Penal code 1860. The tool crimes generally have not required the adoption of new, cybercrime specific laws because they involve using computer technology to commit what is already crime. Such tool crimes are defined in Indian penal code 1860. Whether all the tool crimes are covered by Indian penal code 1860 or some particular tool crimes require modification in the existing law or we need to adopt some new laws. There are number of unpredictable transnational tool cybercrime cases identified as theft, fraud etc. and the judiciary couldn't deal properly with them. The legislators have two options first is to revise the existing definitions of theft, fraud etc. or second to create a new substantive law that encompasses such activities. The first option is preferable as a general matter because it merely updates existing crimes to incorporate the use of new tools. The other option should only be used when absolutely necessary, to avoid an undesirable expansion of criminal law. Unfortunately in India when unbridgeable disparities arise between the scope the existing criminal law and infliction of harm in novel ways by tool cyber crimes, legislatures often have a tendency to adopt new criminal laws that often provide flawed, duplicative or even counterproductive.

* Ass.Prof. School of Law, WU,Ethiopia

[1] http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CC0QFjAA&url=http%3A%2F%2Fwww.wave3.com%2Fstory%2F10629488%2Fhackers-steal-money-from-bullitt-county (Accessed on 18/03/2015)

Proportional transnational approaches to 'physical theft'/ 'virtual theft'

The law defines theft as taking someone's personal property with the intention to steal it. Indian penal code 1860 defines the offence of theft in section 378[2]. Indian criminal law is based on common law. Most of the states who had been colony their criminal law is based on common law principles. For instance many of the U.S. states have statutes that define theft and the definitions are unable to deal with fore fronted technological crimes. According to the criminal law of *"Albama"* theft is knowingly obtain(ing) or exert(ing) control over the property of another, with intend to deprive the owner of his or her property. A few U.S. states also have statutes that define the term "steal". Iowa's criminal law states that "Steal" means to take by theft. Generally theft is defined as taking or carrying away property belonging to another with the intent to deprive the rightful owner to that property. The theft crimes have historically targeted the misappropriation of personal property, rather than real property. As per the law prevailed in U.S. the real property is land and any improvement upon or connected with land. While personal property is any tangible or intangible property, goods, services, chattels, merchandise, commodities, or any item of value in any form or type other than real property. Food gives us energy. In U.K. the common law defines theft only encompassed the misappropriation of tangible personal property, such as gold, jewels and currency. Common law limited theft to tangible property because intangible personal property, as such did not yet exist. Some of the U.S. states define theft in terms of misappropriating tangible or in tangible personal property. But many states have not updated their theft laws so they explicitly criminalize the copying of valuable data[3].

Bank theft without weapons through tool cybercrime:

Higher internet connectivity in Cities has given cyber criminals a bigger platform to play. Unlike in the preceding years, last few years the number of net banking-related crimes have surpassed social media-related complaints. The vulnerability of credit and debit cards and net banking has made it easy for criminals who are just a click away from easy money. Such Crimes are difficult to investigate and also to convict. This is why some of the most trying cases this year belong to this category. Most of the online banking frauds are conducted either through phishing, stealing of banking information or through cloning of credit/debit cards. In phishing, a cyber criminal will send an email pretending to be sent from the bank to the victim asking for their personal details including banking information like PIN code or banking user name and password on some pretext or the other. Once the person reveals such crucial information, the Cyber criminals may withdraw or transfer the money from the account of the victim. In most cases, due to lack of awareness, people fall for the traps of such Cyber criminals and looses huge sums of amount. Some of the cases are difficult to prove in a court of law or even difficult to bring them under the definition of crime. Recently the case of theft through tool cyber has come before the high court of Jharkhand at Ranchi. The case relates to fraud committed in RTGS transactions of money from the State Bank of India, ADB Muzaffarpur Branch, in which the amount of Rs.12.50 crores were transferred from the said Branch to different Banks accounts, out of which, rupees twelve crores was

[2] Indian Penal Code 1860, Section 378 says whoever, intending to take dishonestly any movable property out of the possession of any person without that persons consent, move that property in order to such taking, is said to commit theft.
[3] Susan W.Brenner, Cyber Crime and the Law, Northeastern University Press: New England,Vol1 2012atpage no.57-58

credited into the account of one Maharani Automobiles Ratu Road Ranchi, maintained by HDFC Bank and rupees fifty lakh was credited into the account of Shiva Shakti Traders Bhagwanpur, Muzaffarpur, maintained with the Syndicate Bank. Substantial amount of money was withdrawn after these transactions by the accused persons. The case was instituted against unknown. So far as the role played by the petitioner in these RTGS transactions are concerned, they are detailed in the charge-sheet, which is brought on record. The charge-sheet shows that the petitioner entered into the conspiracy with the co-accused persons, in which the petitioner and the other co-accused were required to manage the connectivity of the SBI network and login ID and password of SBI officials. The petitioner and the other co-accused persons accordingly, managed the device for extending the network of SBI ADB Muzaffarpur Branch, outside the Branch with the help of the wireless device provided by this petitioner. After the fraudulent RTGS transactions to the tune of Rs.12.50 crores were made, the device was removed and the same was again handed over to the petitioner, which was also recovered from the petitioner. [4] The case is still pending before the court. Likewise there are number of tool cyber crimes cases can describe it. The Bullitt County case is a famous case of U.S., in which unknown perpetrators siphoned nearly half a million dollars from the county's bank account. The Bullitt County episode is useful for illustrating how cyber-criminals operate but since no one has been or is likely to be apprehended and charged with stealing the county's funds, it is not particularly useful in analyzing theft as a tool cybercrime.

The First Great Cyber Theft:

The Citibank case may be a best example of theft as a tool cybercrime. In August 1994, Carlos Arario, head trader at the Argentinian firm Invest Capital, came to work one morning and discovered that more than two hundred thousand dollars had disappeared overnight from his firm's account with Citibank. Four anonymous wire transfers had been made from the Invest Capital account to four unknown accounts. Arario called Citibank executives in New York to tell them what had happened. Unfortunately, notwithstanding that call, it continued to happen. In next one month someone siphoned almost ten million dollars from twenty Citibank accounts. Citibank executives assembled in a war room of experts to try to stop the extraction of funds from Citibank accounts, but they could only watch as money was transferred from client accounts to accounts in California, Tel Aviv, Rotterdam, Athens, Latin America, Finland, and Israel. The experts launched a global investigation in an effort to track the transfers and prevent more from occurring. They got a break when the unknown cyber thief transferred $218,000 from an Indonesian businessman's account to a Bank of America account in San Francisco. Citibank experts and federal agents traced the account to Evgeni and Erina Korolkov, Russian nationals who had come to the United States from St. Petersburg. Erina was arrested when she tried to make a withdrawal from the San Francisco account. (She and Evgeni had allegedly opened this and other accounts in order to launder the funds being stolen from Citibank.) Federal agents flew to St. Petersburg and were given access to records that showed the Citibank accounts were being accessed from a computer at AO Saturn, a software company in St. Petersburg. By December, Erina was cooperating with federal authorities and also encouraged her husband to help them identify the Citibank thief. After the FBI promised Evgeni they would treat him leniently if he cooperated, he identified Vladimir Levin, who worked at AO Saturn, as the cyber thief. Levin was then a 29 year old

[4] Banke Buhari Singh vs The State Of Jharkhand on 23 April, 2014 in the high court of Jharkhand at Ranchi, B.A. no.1230 of 2014

computer programmer who allegedly used a laptop computer at the AO Saturn offices to carry out the Citibank fund transfers. As these agents were identifying Levin, other FBI agents were arresting Russian mules in the Netherlands and other countries. The mule's role was to collect the funds that had been transferred from Citibank accounts to foreign accounts. Citibank ultimately claimed it had recovered all but four hundred thousand dollars of the stolen funds.

Since the United States and Russia did not have an extradition treaty, Levin was safe as long as he stayed in Russia. For some reason, he flew to London in 1995, where British authorities arrested him on behalf of the United States. Levin spent eighteen months in a British jail, fighting extradition. He was finally sent to the United States and indicted on federal charges of theft and hacking in 1998. He pled guilty and was sentenced to three years in prison. Many do not believe Levin was the sole architect of the Citibank thefts (or almost thefts). Many found it difficult to believe Levin could have developed and implemented the complex international network of bank accounts and mules to launder the proceeds. Many also did not believe he had the computer skills needed to hack the Citibank accounts. Various theories emerged to explain what really happened. According to one, a Russian hacker group known as Megazoid figured out how to access the Citibank computers. One of them sold that information to Levin or to someone working with Levin for one hundred dollars and two bottles of vodka. As to how Levin implemented the network of international bank accounts and mules, some, including then U.S. attorney general Janet Reno, suggested he was working for the Russian mafia, which was, and is, involved in cybercrime. We will probably never know what happened with the Citibank crimes. Whether Citibank did recover most of the money, whether Levin acted alone in hacking the Citibank system and transferring the funds from the accounts, and whether the Russian mafia was involved, either at the outset or as a broker for the stolen funds. At the time, Citibank confessed that its experts had never quite figured out how the crimes or frustrated crimes were executed. All of that, though, is irrelevant to the point at hand; whoever he was the architect of the Citibank thefts was a post-twentieth-century bank robber. Instead of using a mask and a gun to steal from a bank, he used computers. He used a new tool to commit a very old crime.[5]

Dilemma on Criminal Liabilities in non zero sum thefts:

The notion of theft as a zero sum transfer of property has its roots in English common law, which is the basis of the Indian/U.S. criminal laws. At English common law theft is defined as "the felonious taking and carrying away" element required that the possession of the goods be wholly transferred from rightful owner to the thief[6]. The courts face trouble for convicting cyber criminals in zero sum thefts. Such type of computer theft is straightforward, as far as law is concerned. It is the only type of theft known in the physical world because real-world assets are tangible (e.g., cash, jewels, electronics, etc.). The theft of tangible items is a zero-sum transaction. The possession and use of the items moves entirely from the rightful owner to the thief. Since this is the only type of theft that can occur in the real world, theft laws tend to assume zero-sum theft. It is not the only type of theft that can occur once property becomes intangible. Certain types of computer data have great value, but data is intangible; unlike property in the real world, digital property is not an either-or commodity. That is, it does not

[5]Internet Fraud Case City Bank Vladimir Levin, at www.cab.org.in/Lists/Knowledge%20Bank/Attachments/64/InternetFraud-VL.pdf (Accessed on 20/03/2015)
[6] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO: Vol1 2010 at page no.158

by definition; exist in only one place at a time. Digital property can be duplicated, which means it can exist in two (or more) places at the same time.[7]

State v. Schwartz Case: That aspect of digital property was at issue in Oregon. Oregon is a state in northwestern United States on the Pacific. In the said case Randal Schwartz was an independent contractor working for Intel Corporation. At one point, he began working in Intel's Supercomputer Systems Division (SSD), which created "large computer systems" that were "used for applications such as nuclear weapons safety." Everyone who worked at SSD had to use a unique password to gain access the SSD computers and the data stored on them. The data was stored "in an encrypted or coded fashion." After he had worked there for a while, Schwartz had a disagreement with a systems administrator that led to the termination of his contract with SSD. (Schwartz later said he hadn't left SSD on the best of terms.) Intel disabled his passwords for all but one of the SSD computers. It inadvertently failed to disable his password for the computer known as Brillig. Schwartz continued to work as a contractor for a different Intel division and accessed the Brillig computer without being authorized to do so. About a year and a half after he quit working for Intel's SSD division, Schwartz downloaded a password guessing program called Crack. When he ran Crack on Brillig, he discovered the password for "Ron B". One of Brilligs authorized users. Although he knew he did not have the authority to do so, (Schwartz) used Ron B's password to log onto Brillig. From Brillig, he copied the entire SSD password file onto another Intel computer, Wyeth. Once the SSD password file was on Wyeth, (he) ran the Crack program on that file and learned the passwords of more than 35 SSD users, including... the general manager of SSD. Apparently, (Schwartz) believed that, if he could show SSD's security had gone downhill since he left, he could reestablish the respect he had lost when he left SSD. Finally Schwarz got the opportunity and he stole all the data. Schwartz held liable not because of being charged under a regular theft statute, but he was charged with violating a statute that made the theft of information a crime. The court of appeals was able to use the fact that this statute was designed to protect information to rationalize what was problematic the notion of non-zero-sum theft of property. If the charge had been brought under the regular theft statute, it would have been difficult for the court of appeals to uphold Schwartz's conviction.

Oregon's theft statute, like Indian theft statutes, defines the crime in terms of "depriving" someone of their property."Deprive" is defined as "to deny... possession" of something.[22] This notion of theft as a complete transfer of property has its roots in English common law, which is the basis of Indian Criminal Law as well as U.S. Criminal Law. In common law, theft was defined as "the felonious taking and carrying away of the personal goods of another." The "taking and carrying away" element of the crime required that the possession of the goods be completely transferred from the rightful owner to the thief. Section 378 Indian penal code requires the movement of moveable property from owner to the person who is not legally entitled. that would therefore have been more difficult for the Oregon Court of Appeals to uphold the conviction if it had involved a traditional zero-sum theft charge.

The *Schwartz* case[8] illustrates not only how theft can become a tool cybercrime but also why governments need to revise their laws so they encompass new variations of old crimes. One

[7] Graham Davies, Anthony Beech (Editors),Forensic Psychology crime, justice, Law Interventions, ,British Psychological society and john wiley and sons Ltd.: UK, Second Edition, 2012 at Page no. 227

approach some states have taken is to expand the definition of "deprive" as the word is used in theft statutes. In Delaware theft statutes, for example, deprive means "to withhold property of another person permanently or for so extended a period or under such circumstances as to withhold a major portion of its economic value or benefit." The last option captures the kind of non-zero-sum data theft that was at issue in the Schwartz case. In Indian case laws such thefts are not distinguished frequently. In case A. Shankar vs State It is alleged by the prosecution that on 01.04.2008 and 02.04.2008 at the room of Legal Advisor's of Directorate of Vigilance and Anti-Corruption (DVAC), Chennai A. Shankar being a Special Assistant of Confidential Section in Directorate of Vigilance and Anti-Corruption office, functioning at NCB-23 building with intent to cause damage to the office of the Directorate of Vigilance and Anti-Corruption, which has not considered his appointment to the Secretariat as Assistant Section Officer (ASO), without the permission of the owner of the computer i.e., the witness Thiru N.Vijayarajan, Legal Advisor of DVAC and authorised user of the computer, having taken advantage of the absence of Legal Advisor, unauthorisedly accessed into the computer system of Legal Advisor through his pen drive named "SUJATHA" accessed the folder "Director's back up 2" kept in the Legal Advisor's computer without the permission of the owner of the information i.e., witness Thiru S.K.Upadhyay, and also downloaded the audio file including "CS 20.09.2007" and caused publication of the same in the "Deccan Chronicle" an English daily news paper on 14.04.2008 and also for the telecast on the same day on "Makkal TV" and "Jaya TV" at 08.00pm and 10.00pm., respectively. The petitioner by accessing the computer system and information without the permission of the owners/authorised users copied, caused publication and thereby diminished the value of information, utility and affected it injuriously by means of securing access and downloaded the information, which was recorded and saved for the purpose of exclusive possession and use by the witness Thiru S.K.Upadhyay. It is also alleged that the A.shanker had secured access unauthorisedly to the protected system of the Legal Advisor (notified under G.O.Ms.No.5 & 6 of Information Technology Department dated (29.06.2005). On the above said dates through his pen drive names "SUJATHA" and downloaded the information, which was created for the purpose of exclusive possession and use by the witness Thiru S.K.Upadhyay in contravention of Section 70 of Information Technology Act 2000 and hence after filing of the charge sheet on 26.12.2008, now the A.shanker for the alleged commission of offences of hacking with protected computer system and breach of confidentiality has been facing three charges under Sections 66, 72 and Section 70 of Information Technology Act 2000. Petitioner A.shanker filed a petition under Section 482 Cr.P.C, praying to quash the charge sheet. The one of the arguments was based on non zero sum theft. The case was dismissed by the Madras High Court. [9]

Theft of trade secrets/ stealing confidential information by employee:

Unlike U.S. and other developed countries Indian has no legislation dealing with trade secrets. Being a signatory of the TRIPs agreement India is under an obligation to bring intellectual property law in conformity with international standards in this regard. India has achieved it up to some extent by enacting new laws and by amending existing legislation. In India protection of trade secrets from theft is based on precedents. However section 27 of the

[8] Susan W.Brenner, Cyber Crime and the Law, Northeastern University Press: New England,Vol1 2012atpage no.63-68

[9]A. Shankar vs State Rep. decided on 13 December, 2010 by IN THE HIGH COURT OF JUDICATURE AT MADRAS.

Indian contract Act provides some sort of limited remedy. On the conterary the federal criminal code of U.S. approaches the theft of proprietary information or trade secrets as economic espionage. The Economic Espionage Act of 1996 (EEA) criminalized two types of trade secret theft i) Section 1831 of Title 18 of the U.S. Code makes it a crime to steal a trade secret to benefit a foreign government. This offense is analogous to the traditional crime of espionage, since it is committed on behalf of another nation-state. ii) Section 1832 of Title 18 of the U.S. Code criminalizes the theft of trade secrets that is "carried out for economic advantage regardless of whether it benefits a foreign government or foreign agent.

The Indian statutes don't define the trade law significantly but section 2(3) of the Indian innovation bill defines "confidential information". "Confidential information" means information, including a formula, pattern, compilation, program device, method, technique or process……." . In U.S. the EEA defines "trade secret" as (1) "financial, business, scientific, technical, economic, or engineering information,... whether tangible or intangible" (2) that is "stored, compiled, or memorialized... electronically, graphically,... or in writing" (3) if the owner took "reasonable means" to keep the information secret and (4) if it "derives independent economic value" from not being "generally known to" or "readily ascertainable" by the public. When the act was adopted in 1996, online economic espionage was not a notable concern, but it has become a major concern in the years since, as a New York prosecution illustrated. The case of Sergey Aleyniov is a landmark case of this issue and the U.S. government had to change the law. On July 3, 2009, he was arrested by FBI agents at Newark Liberty International Airport after Goldman raised the alarm over a suspected security breach. He was accused by the FBI of improperly copying computer source code that performs "sophisticated, high-speed and high-volume trades on various stock and commodity markets", as described by Goldman. The events leading to his arrest are covered by Michael Lewis in his 2014 book *Flash Boys*.[10] According to Assistant United States Attorney Joseph Facciponti, "the bank has raised the possibility that there is a danger that somebody who knew how to use this program could use it to manipulate markets in unfair ways."[11] Aleynikov acknowledged downloading some source code, but maintained that his intent was to collect open-source code. As this is a common practice among programmers, this is notoriously difficult to prove. In June 2010, Aleynikov filed a motion in the Federal Court to dismiss the indictment for failure to state a claim. He argued that the acts he was accused of didn't constitute a crime. The Federal Judge Denise Cote dismissed one charge against him but denied the rest of the motion. In December 2010 Aleynikov had a jury trial in the United States District Court for the Southern District of New York, where the courtroom was sealed to public access several times. On December 10, he was convicted of the two counts of theft of trade secrets and transportation of stolen property.[12] Later he was sentenced to 97 months (8 years) in prison, three years of supervised release following his prison sentence, and a $12,500 fine, despite the recommendation of the Federal Probation Service of suggesting a 24 month (2 years) sentence.[13] Three weeks before sentencing, Aleynikov was incarcerated on

[10] Lewis, Michael (2014). *Flash Boys: Cracking the Money Code*. London, UK: Allen Lane. ISBN 9780241003633.
[11] David Glovin and Christine Harper (July 6, 2009). "Goldman Trading-Code Investment Put at Risk by Theft (Update3)". *Bloomberg*. Retrieved August 10, 2012.
[12] Peter Lattman (December 10, 2012). "Former Goldman Programmer Found Guilty of Code Theft". *The New York Times*. Retrieved August 10, 2012.
[13] Bill Singer (March 22, 2011). "Former Goldman Sachs Programmer Sentenced in Federal Criminal Case". *Forbes*. Retrieved August 10, 2012.

request of the government, as he was judged to be more of a flight risk after separating from his wife. In March 2011, Aleynikov appealed the conviction, asking the Second Circuit to review the District Court's decision denying his original motion to dismiss the indictment for failure to state a claim.[14] On February 16, 2012, the United States Court of Appeals for the Second Circuit heard oral argument on his appeal and, later that same day, unanimously ordered his conviction reversed and a judgment of acquittal entered, with opinion to follow.Aleynikov was released from custody the next day. On April 11, 2012, Dennis Jacobs, Chief Judge of the United States Court of Appeals, published a unanimous decision in a written opinion stating[15]:

On appeal, Aleynikov argues, *inter alia*, that his conduct did not constitute an offense under either statute. He argues that: (1) the source code was not a "stolen" "good" within the meaning of the NSPA, and (2) the source code was not "related to or included in a product that is produced for or placed in interstate or foreign commerce" within the meaning of the EEA. We agree, and reverse the judgment of the district court.[16] To understand why online economic espionage is such a concern, it is only necessary to imagine a slightly altered version of the facts alleged in the *Aleymkov* case: assume, for the purposes of analysis, that Aleynikov copied the Goldman Sachs source code and transferred the data to the German server. Now assume that instead of staying in the United States to take a position with Teza (or some other company), Aleynikov immediately went to the airport and boarded a flight for Russia. The United States does not have an extradition treaty with Russia; therefore, Russia would not be obliged to turn him over to U.S. authorities so he could be returned to the United States and tried on the economic espionage charge. In this scenario, Aleynikov would be safely ensconced in a foreign country, immune from U.S. justice and the source code would become a commodity that could be sold to the highest bidder.

Criminalization of theft of services:

Data theft is not the only tool cybercrime involving theft, at least not according to some. In a number of instances, people have been charged with theft based on their using wireless Internet networks provided by businesses libraries and other institutions. In 2006, twenty-year-old Alexander Eric Smith of Battle Ground, Washington, was charged with theft after he parked his truck in the parking lot of a coffee shop (Brewed Awakenings) and used its wireless network. Smith was charged after Brewed Awakenings employees called the police to report that he had been using the shop's wireless network for three months (without ever buying anything).

Smith and other wireless freeloaders are charged with "theft of services," a crime that until recently only encompassed obtaining telephone, electricity, cable, and professional services without paying for them.[37] Theft of services is a relatively new crime. In common law, "time or services" were not "recognized as a subject" of theft because there can be no "taking and carrying away" of either. "The criminalization of the theft of services in the United States began in the 1960s as a result of the American Law Institute's Model Penal Code.[59] The

[14] "United States v. Aleynikov". United States Court of Appeals for the Second Circuit. April 11, 2012. Retrieved August 10, 2012.
[15] Kim Zetter (April 11, 2012). "Code Not Physical Property, Court Rules in Goldman Sachs Espionage Case". *Wired*. Retrieved August 10, 2012.
[16] "United States v. Aleynikov". United States Court of Appeals for the Second Circuit. April 11, 2012. Retrieved August 10, 2012

Model Penal Code which, as its name implies, is a template for drafting criminal statutes appeared in 1962 and introduced a new theft of services crime.'[10] Under the Model Penal Code, one commits theft of services if he obtains services "he knows are available only for compensation" without paying for them. Services include "labor, professional service, transportation, telephone or other public service, accommodation in hotels, restaurants or elsewhere, admission to exhibitions, (and) use of vehicles or other movable property." The Model Penal Code's theft of services crime which has been adopted by most, if not all, states[41] differs slightly from traditional theft crimes. Traditional theft is a zero-sum event in which the possession and use of property is transferred from one person (the owner) to another (the thief); if the thief succeeds, the victim is completely deprived of her or his property In theft of services, the victim's property is the ability to offer services in exchange for pay When a theft of services occurs, the victim is completely deprived of some quantum of the services she or he offers or, more accurately, of the remuneration that should have been paid for those services but is not deprived of the ability to offer such services. This difference is irrelevant to the applicability of traditional principles of criminal liability because the victim has still been deprived of a commodity that lawfully belonged to her or him[17].

When the Model Penal Code was written, there was no Internet and no wireless Internet access. But there is no reason the theft of services crime cannot apply to free loading on a wireless network; if nothing else, the theft of wireless services comes within the Model Penal Code's definition of services as including "telephone or other public service." The only real difficulty with applying theft of services to wireless freeloading comes with another aspect of the crime: the requirement that the person being charged knew the services were "available only for compensation." When someone taps an electric line to get free electricity, she or he *has* to know that the service is legally available only to those who pay for it; if nothing else, we can infer the person's knowledge from the fact that she or he surreptitiously tapped into the electric company's lines and that it is common knowledge one must purchase electricity, just as they purchase other commodities. The same logic applies when someone obtains other services such as telephone or television cable service because he or she cannot obtain those services without doing something to bypass conduits or other devices intended to make the service available only to those who pay for it.[18] The problem that can arise in applying theft of services to wireless free-loading is that wireless Internet service, unlike other services, is sometimes given away for free. In the Smith case, the coffee shop was intention-

Evalution:

Cyber theft has become rampant around the world today and has become one of the fastest growing crimes of this century. In India the parliament has passed a new law to deal with cyber related thefts which is defined as identity theft in information technology act 2000. It occurs when someone uses another person's personal information, such as name, credit card number, bank account details, address, or other identifying information to take on that person's identity, in order to commit financial fraud or other crimes. The crime of identity theft is not limited to online transactions or online banking but the scope of such crime is very vast. Stealing an identity is, unfortunately, surprisingly easy to do and happens when one can least expect it. If the cyber criminal steals the identity it can take months or even

[17] Anupa p Kumar, Cyber Law, Published under the banner of YFI and Anupa P kumar: Bangalore,Vol 1 2009 at page no. 25
[18] Ibid at page no. 27

years to recover from the disorder they leave behind, Though we have a traditional definition of theft taken by common law country. We have developed our new cyber law but still study shows a bigger share property victimization related to tool cyber crimes. Even with the reducing number of cases, the value of such cases did not come down proportionately. Banking cyber frauds in the country are the result of introductory phase of banking technology like ATM, online banking, mobile banking, EFT etc. which need time for people, market and technology to get matured. Regulatory legal framework will also get stronger by practical experience only.