**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2013, Volume 2, Issue 1, pp. 42-50, Article ID Tech-160
ISSN 2320 – 0235

Research Article | Open Access

# Comparative Analysis of Trends of Cyber Crime Laws in USA and India

**Rajlakshmi Wagh**

IMED, Department of Management, Bharati Vidyapeeth IMED, Pune, Maharashtra, India

Correspondence should be addressed to Rajlakshmi Wagh, rajlakshmi@wagh.org

Publication Date: 9 December 2013

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-160



**Abstract** Today's Global era needs laws governing fast paced cyber crime. The popularity of on-line transaction is on the rise thereby having attempts made by unscrupulous entities to defraud internet users. The modus operandi may be in the form of Hacking, Spoofing, Pornography, Scanners, Device, Fake card and the like. The Educational sectors, Defense sector, Law Enforcement Bodies, Bank sectors are exposed to risk as the information sought usually includes data such as username, passwords, bank account and credit card number, revelation of which is huge loss for not only every individual but also the state at large. The paper is an analysis of the USA Laws for Cyber Crime with a comparative analysis with the Indian Laws. The aim is to analyze the conviction rate in cyber crime with comparison to both the countries and suggest various remedies.
**Keywords** *Statutes; Offences; Sections; Conviction*

## 1. Introduction

The challenges faced by cyber laws are vast due to geographical hurdles, cultural patterns and land laws governing one's particular land. Easy access to cyberspace is one of the main reasons for the growth of cyber crime thereby threat to the National security of the country. There exists a dearth of adequate laws. According to NASSCOM, there is extremely low rate of conviction of cyber crime in India. It saddens to say that India as a country in its 10 years old history of cyber crime investigation has so far witnessed only four convictions.

The statistics show that 1600 have been arrested against 3682, where the conviction is shocking 7 of which 3 are significant. To look into more detail the number of crime has gone up by 10 fold. I would like to bring to the notice that such a rise in the crime is due to low rate of conviction rate [1]. In the year 2007, the arrests made were 154 while in the following year there was 178. In the years 2009 and 2010, the numbers of persons arrested were 288 and 799 and in 2011, it was 1,184. This shows clearly a huge rise in the number of arrests but yet a single digit conviction rate [2]. A further record

also show that 217,288, 420,966 and 1,791 cyber crime cases were registered under IT Act, 2000 during the years 2007, 2008, 2009, 2010 and 2011.

## 2. Overlook of Some of the Cyber Crime Affected States in India

In Karnataka 307 cases of cyber crime were booked in the last 9 years and only 60 of them have been charge sheeted and not seen a single case of conviction in cyber crime [3]. According to State Criminal Investigation Department (CID) statistics, the conviction rate is 8.2 per cent, which means it has achieved in only nine out of 100 cases [4].

## 3. An Overview of Some of the Status of Convictions in India

The first conviction came in through the Sony India Private limited case. The complaint was filed by Sony India Private Limited which used to run a website sony-sambandh.com which enabled NRIs to send Sony products to India. On this site a colour television was ordered and the payment was made through a credit card. The product was to be delivered to Noida and all procedures had been followed. However two months later the credit card said that this was an unauthorized transaction following which a case of cheating was filed with the CBI. On investigation it was that the person who received the television set had gained access. Before court the crime was admitted and the accused was convicted. However the court released the accused on probation for a year since he was only 24 years old [5].

## 4. An on Look of Conviction Rate in the USA

A total of 145 cases against 243 defendants were also terminated during the year, representing an eight percent decrease in cases terminated and 19 percent increase in defendants terminated when compared to the prior year. Eighty-six percent of all terminated defendants were convicted, with 61 percent of the convicted defendants sentenced to prison. This data represents only those cases and defendants charged directly under the federal computer intrusion statute, 18 U.S.C. § 1030, and the provisions regarding stored electronic communications, 18 U.S.C. §§ 2701-2711 computer intrusion cases involving financial loss are often charged under the federal fraud statutes, and other intrusion cases may be brought under the federal identity theft statute, 18 U.S.C. § 1028.

The number of complaints registered with Internet Crime Control Centre (IC3) of the USA from 2006, 2007, 2008, 2009, 2010, 2011 are 207,492; 206,884; 275,284; 336,655; 303,809; 314,246 [6]. This also shows the awareness of cyber laws among the Americans.

A detail study of the Cyber law legislation in America show a listing of various statutes from 1970 till date.

### 4.1. US Cyber Crime Laws: An Exordium

**The Wire Fraud Statute** being the first law used to prosecute computer criminals in the USA. It was seen that the communication wires were used in international commerce to commit fraud. To overcome such US passed the Law so as to prohibit the use of communication wires. This was an effective statute as it was to overcome defrauders trying to obtain money, property by false representation or promise; modus operandi being radio or television communication, signs or signals [7]. This statute was successfully used in 1970's and 1980's to convict government officials of defrauding the public of its intangible right [8]. In a paradigmatic case Governor Marvin Mandel of Maryland was convicted of mail fraud for promoting certain legislation beneficial to the owners of a race in violation of his obligation to render the citizen of the state fair and impartial service free from bribery [9].

The era witnessed technological progress so this Statute suffered certain limitations the wire fraud statute was written without computer crime in mind and as such it has serious limitations when dealing with it, not all computer related crimes can be prosecuted with it, not every crime committed using a computer is done with the intent to commit a fraud, and not all computer crimes use interstate or international wires [10]. A need for a more effective law namely **The Computer Fraud and Abuse Act CFAA** – 1984 and amended in 1986. This being one of the most important statute as it deals with computer crime. The main reason for it to be amended in 1994 was that it could deal with the problem of "Malicious Code" such as viruses, worms and other programs which are designed to destroy data on a computer. The Act suffered major lacunae as it could not prosecute those who transmitted programs with intent to cause damage to the computer [11].

The National Information Infrastructure Protection Act was created to further expand the protections granted by the Computer Fraud and Abuse Act of 1986. Under the new act, protective measures were extended to computer systems used in foreign and interstate commerce and communication. The bill consolidated several older laws, including standing espionage laws, and labeled new crimes for stealing classified information from government computers [12]. CFAA is also known as Title 18 U.S.C Section 1030. NIIA made it illegal to view information on computer without authorization [13].

In 1986 the Electronic Communication Privacy Act (ECPA) was amended making it illegal to intercept stored or transmitted electronic communication without authorization. It prohibited illegal access and certain disclosures of communication contents. Later on amended in 1994 [14]. The CSEA (Cyber Security Enhancement Act) was passed together with Homeland Security Act in 2002. This Act granted powers to the law Enforcement Organizations and increased penalties set out in the Computer Fraud and Abuse Act [15]. The Act authorizes harsher sentences for individuals who knowingly or recklessly committed a computer crime that resulted in death or serious bodily injury.

## 5. Other Laws for Computer Crime Prosecution

EEA Economic Espionage Act passed in 1996. To stop trade secret misappropriation. There being other Statute namely National Stolen Property Act and Virginia Internet Policy Act comprising of 7 bills. The proposed Computer Crime Legislation namely,

FOISA – Fraudulent Online Identity Sanction Act, registering online domain under false identification, increase jail time to provide false information.

CSPCA – Computer Software Privacy and Control Act, to deal with eighth problems of spyware. When passed it would prohibit transmission of software that collects and transmits personal information about the owner or operator of the computer.

The US legal system is and always more tech savvy and specialized to tackle various issues. In case of credit Card Fraud in USA there is a separate Federal Credit Card Law that stipulates the consumer. The Fair Credit Billing Act (FCBA) will apply to billing errors on credit card, unauthored charges, charges for goods and services. This Act is an attempt to minimize Credit Card Fraud in India.

## 6. Laws Governing Cyber Crime in India

The Information Technology (Amendment) Act 2008 is the only Legislation that governs cyber crime in India. Till date it has brought various sweeping changes. The various sections that have been amended are Section 66 A - An offence to send offensive messages, Section 66B – An offence to receive stolen computer resource. Section 66C, 66D, 66E & 67F are inserted to declare identity theft, cheating and percolation, violation of piracy, video voyeurism and cyber terrorism and such which are

punishable under the IT Act. The section 67A, 67B & 67C which provides punishment of imprisonment of three years and fine for acts such as, child pornography.

## 7. Civil Wrong

Section from 43 to 47 tackles the civil liability of individuals. The liability is to the extent of damages. The quantum of compensation is decided by the adjudicating officer as he has jurisdiction to adjudicate such claims which does not exceed Rupees five Crore. Section 64 provides for recovery of penalty as arrears of land revenue for the suspension of license or Digital Signature Certificate till penalty is paid.

## 8. Criminal Wrong [16]

| | |
|---|---|
| Section 65 –Tampering with computer Source Documents, imprisonment up to 3 years or fine which may extend to two lakh rupees or both. | Sec 66E – Punishment for violation of privacy, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or both. |
| Sec 66 – Computer Related Offences with reference to section 43, punishable with imprisonment for a term which may extend to 3 years or with fine which may extend to five lakh rupees or both. This section has reference to IPC for some definitions. | Sec 66F – Punishment for cyber terrorism, shall be punishable with imprisonment which may extend to imprisonment for life. |
| Sec 66A – Punishment for sending offensive messages through communication service, punishable with imprisonment for a term which may extend to 3 years and with fine. | Sec 67 – Punishment for publishing or transmitting obscene material in electronic form. |
| Sec 66B – Punishment for dishonestly receiving stolen computer resource or communication device. | Sec 67A – Punishment for publishing or transmitting of material containing sexually explicit Act shall be punished on first conviction with imprisonment for a term which may extend to five years and with fine which may extend to ten lakh rupees and further punishment on subsequent conviction. |
| Sec 66C – Punishment for identity theft, punishment with imprisonment which may extend to 3 years and liable to fine which may extend to one lakh rupees. | Sec 67B – Punishment for publishing material depicting children in sexually explicit act in electronic form shall be punishable on first for a term to five years and with a fine which may extend to ten lakh rupees and for subsequent offence, punishment for term which may extend to seven years and also with fine which may extend to ten lakh rupees. |
| Sec 66D – Punishment for cheating by personating by using computer resource, punished with imprisonment which may extend to three years and shall be liable to fine which may extend to one lakh rupees. | |

## 9. There are Other Offenses Covered Under IPC and Special Laws

| | |
|---|---|
| Sec 503 – Sending threatening messages by email | Sec 464- False document |
| Sec 499 – Defamation | Sec 468 – Forgery for cheating |
| Sec 463- Forgery | Sec 469 – Forgery for purpose of harming reputation |

- **Bogus Website, Cyber Frauds**

Sec 420 – IPC Cheating and dishonestly inducing delivery of property.

- **Web – Jacking**

Sec 383 IPC Extortion

- **Email Abuse Online Defamation**

Sec 500 – Punishment for defamation
Sec 509 IPC Word gesture or act to insult modesty of women.

- **Criminal Intimidation by E-Mail or Chat**

Sec 506 – Punishment for criminal intimidation
Sec 507- Criminal Intimidation by an anonymous communication

- **Online Sale of Drugs, NDPS Act**
- **Online Sale of Arms Act**
- **Piracy – In Copyright Act**

Sec 51, Sec 63, Sec 63 B

- **Obscenity**

Sec 292 – Sale of obscene books
Sec 292- A printing of grossly indecent matter for blackmail
Sec 293- Sale of obscene objects to young persons.
Sec 294 – Obscene acts 7 songs.
Section 378. Theft
Section 379. Punishment for theft

**The Indian Evidence Act 1872** is another legislation amended by the ITA. Earlier to the passing of ITA, all evidences in a court were in the physical form only. By the passing of the ITA it gave recognition to all electronic records and documents as subsequent amendments were made to The Indian Evidence Act. Words like 'digital signature', 'electronic form', 'secure electronic record' information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations [17].

**The Bankers' Books Evidence (BBE) Act 1891 has been** amended. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits. With the passing of the ITA the definitions part of the BBE Act stood amended.

**The Anti Money Laundering Act 2002** having its main objective to for confiscation of property derived from, or involved in, money laundering.

**The Critical Information Infrastructure Protection (CIIP)** the Central Government being empowered to appoint a National Nodal Agency responsible for all measures including research and development [18].

## 10. Status of Persons Arrested as against Cases Registered in India

The table below shows a list of cyber crime for the past 5 years from 2009 to 2011. A Crime wise statistical report of increase in crime and also persons arrested. Source NCRB [19].

| Sr. No. | Crime Head under IT. Act | Cases Registered from 2009 Onwards | | | | Persons Arrested | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 08 | 09 | 10 | 11 | 08 | 09 | 10 | 11 |
| 1. | Tampering computer source documents | 26 | 21 | 64 | 94 | 26 | 06 | 79 | 66 |
| 2. | Hacking with Computer System i) Loss/damage to computer resource/utility 109.0. (ii)Hacking | 56 | 115 | 346 | 826 | 41 | 63 | 233 | 487 |
| | | 82 | 118 | 164 | 157 | 15 | 44 | 61 | 65 |
| 3. | Obscene publication/transmission in electronic form | 105 | 139 | 328 | 496 | 90 | 141 | 361 | 443 |
| 4. | Failure (i) Of compliance/orders of Certifying Authority ii) To assist in decrypting the information intercepted by Govt. Agency | 1 | 3 | 2 | 6 | 1 | 2 | 6 | 4 |
| | | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 5. | Un-authorized access/attempt to access to protected computer system | 3 | 7 | 3 | 5 | 0 | 1 | 16 | 15 |
| 6. | Obtaining license or Digital Signature Certificate by misrepresentation/suppression of fact | 0 | 1 | 9 | 6 | 11 | 0 | 1 | 0 |
| | Publishing false Digital Signature Certificate | 0 | 1 | 2 | 3 | 0 | 0 | 0 | 1 |
| | Fraud Digital Signature Certificate | 3 | 4 | 3 | 12 | 3 | 0 | 6 | 8 |
| | Breach of confidentiality/privacy | 8 | 10 | 15 | 26 | 3 | 3 | 5 | 27 |
| | Other | 4 | 1 | 30 | 157 | 0 | 0 | 0 | 68 |
| | **Total** | 288 | 420 | 966 | 1791 | 154 | 178 | 288 | 1184 |

From the above table it is seen that the cyber crime criminals arrested is 50% less overall, showing that the law enforcement agency should mold themselves to the fast paced cyber crimes and the effective Legislations.

## 11. Conclusions

Legislations in other nations as against the lone legislation ITA and ITAA in India, in USA there are many legislations governing e-commerce and cyber crimes going into all the facets of cyber crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act.

In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records. Companies dealing with US firms ensure HIPAA compliance insofar as the data relating to such corporate are handled. The Sarbanes-Oxley Act (SOX) signed into law in 2002 and named after its authors Senator Paul Sarbanes and Representative Paul Oxley, mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

Besides, there are a number of laws in the US both at the federal level and at different states level like the Cable Communications Policy Act, Children's Internet Protection Act, Children's Online Privacy Protection Act etc. In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc are all regulatory legislations already existing in the area of information security and cyber crime prevention, besides cyber crime law passed recently in August 2011.

In India the government has taken steps in the framing of The National Cyber Security Policy. This policy proposes to

a) Facilitate collaboration between government agencies and private cyber security solutions developers in order to optimize and protect critical government initiatives

b) The policy is a road map for strengthening cyber security as it will secure a computing framework that will inspire consumer confidence for electronic transaction.

c) At the macro level the policy will facilitate cyber security intelligence that will form an integral component to anticipate attacks and quickly adopt counter measures.

The Central and the State Government have been authorized to issue directions for interception or monitoring or decryption of any information through any computer resource. Both the governments, in the interest of sovereignty or integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, may intercept, monitor or decrypt or cause to intercepted, monitored or decrypted any information generated, transmitted received or stored in any computer resource. They can block public access to any information through any computer resource.

Dream to keep the society crime-fee will remain a dream in India as there should be constant endeavor for the legislation to keep in pace with the fast pace in crimes. Especially in a society that is dependent more and more on technology, crime based and electronic offences are bound to increase and the law makers have to go the extra mile keeping in pace to the fraudsters as technology is always a double-edged sword and can be used for both the purposes – good or bad.

We can conclude that though the cyber police have become proactive but the rise in the number of instances may be due to weak law and to have appropriate legislations for the fast track crime. To suggest Fast Track courts to be set up to keep in pace with the giga second of commission of cyber crime.

The government has set up cyber crime cell in various states of India yet the need to have well trained Law Enforcement bodies so they do not find it difficult to defend their cases in the court of law. The need is felt to have expertise personnel police who could specialize to handle cyber crime. These cyber crime offences are bailable offences leading to the lack of confidence in the laws.

## References


[1] Rediff.com, Dec, 2012. http://www.rediff.com/business/report/tech-cyber-crime-1600-arrested-only-7-convicted/20121211.htm

[2] NCRB Report. http://www.rediff.com/money/report/tech-cyber-crime-1600-arrested-only-7-convicted/20121211.htm

[3] indlaw.com (The Definitive Guide to Indian Law), 1997-2013. www.indlaw.com/guest/Displaynews.aspx?indlaw.com

[4] PuneMirror.in, 24th Nov., 2012: Rate of Conviction Shows Decrease, Cyber Crime Up. Bennett Coleman & Co. Ltd. http://www.punemirror.in/article/2/20121124201211240823554 8196c927a5/Rate-of-conviction-shows-decrease-cyber-crime-up.html?pageno=9

[5] National Crime Records Bureau (Ministry of Home Affairs). http://ncrb.nic.in.

[6] Internet Crime Complaint Center. 2011 Internet Crime Report. http://www.ic3.gov/media/annualreport/2011_ic3report.pdf

[7] Legal Information Institute (LII). 18 USC 1343-Fraud by Wire, Radio, or Television. 1988. 113-36.

[8] Aaron. D. Hoag. *Defrauding the Wire Fraud Statute: United States v La Macchia*. Harvard Journal of Law and Technology. 1995. 8 (2) 511.

[9] Aaron. D. Hoag, Defrauding The Wire Fraud Statute: States v. Mandel, 591 F.2d 1347, 1360 n.7 (4th Cir. 1979), cert. denied, 445 U.S. 961 (1980). Harvard Journal of Law and Technology. 1995.

[10] Maxim May, Fedral Computer Crime laws, SANS Institute: Reading Room Site. June 1, 2004, 2.

[11] Maxim May, Fedral Computer Crime laws, SANS Institute: Reading Room Site. June 1, 2004, 2.

[12] National Information Infrastructure Protection Act, United States, Gale Encyclopedia of Espionage & Intelligence, 1. http://www.answers.com/topic/national-information-infrastructure-protection-act-united-states

[13] Maxim May, Fedral Computer Crime Laws, SANS Institute: Reading Room Site. June 1, 2004, 3.

[14] Maxim May, Fedral Computer Crime laws, SANS Institute: Reading Room Site. June 1, 2004, 5,

[15] 99th Congress. Electronic Communications Privacy Act (ECPA). Public Law 99-508. October 21, 1986. Retrieve on May 24, 2000. http://www.cpsr.org/cpsr/privacy/communications/wiretap/electronic_commun_privacy_act.txt.

[16] Maxim May, Fedral Computer Crime laws, SANS Institute: Reading Room Site. June 1, 2004, 6.

[17] Ministry of Law, Justice and Company Affairs (Legislative Department), 9th June 2000: The Information Technology ACT, 2008. New Delhi.

[18] NCRB, Chapter 18. Cyber Crimes. http://ncrb.nic.in/CD-CII2011/cii-2011/Chapter%2018.pdf.

[19] Ministry of Law, Justice and Company Affairs (Legislative Department) Section 69, Information Technology (Amendment) Act 2008. New Delhi.