Cyber Crimes in India: A Study

Dr. Malabika Talukdar

[B.A(H), LL.M, Ph.D]

Assistant Professor, University Law College, Gauhati University. Guwahati-14, Assam, India

E-mail: malabikatalukdar11@gmail.com

ABSTRACT:

Cyber crime means that criminal activity where a computer or network is the tool, source or target. In other words, cyber crime can be described as the criminal use of computer technology. The Dictionary meaning of cyber crime is that it is those crimes which are committed with the help of computers or relating to computers, mainly through internet. Crimes involving use of information or usage of electronic means in furtherance of crime are covered under the scope of cyber crime. Cyber Crimes may be committed against persons, against property and against government. Success and amazing advancement in any field of human activity leads to crime that needs mechanisms or regulations to control it. There should be stringent legal provisions for combating cyber crimes which could provide assurance to bonafied users along with empowering law enforcement agencies and deterrence to criminals in the concerned field.

Therefore, in this paper I'll try to find out the different forms of cyber crimes existed in our country and will try to provide certain remedial measures which will certainly be helpful for combating this societal evil.

KEYWORDS:

Cyber Crime; Computer; Computer Technology; Enforcement Agencies; Information; Internet; Network

1. INTRODUCTION

Day by day the use of computer is increasingly & more users are connecting to the internet. So the crimes are also increasing. But mostly peoples are unaware about cyber crimes. Although the term

cybercrime is usually restricted to describing criminal activity in which the computer or network is an essential part of the crime. Cyber Crimes are defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails,) and mobile phones (SMS/MMS)". Such new crimes devoted to the Internet are email "phishing", hijacking domain names, virus imitation, and cyber vandalism.[1]

Crime is both a social and economic phenomenon. It is as old as human society. Many ancient books right from pre-historic days, and mythological stories have spoken about crimes committed by individuals be it against another individual like ordinary theft and burglary or against the nation like spying, treason etc. Kautilya's Arthashastra written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken by the rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it.[2]

1.1 What is Crime?

Crime in any form adversely affects all the members of the society. In developing economies, cyber crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitization of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that man cannot spend a day without computers or a mobile. Snatching some

[1] A Study of Cyber Crimes & Cyber Laws In India by PARDEEP MITTAL & AMANDEEP SINGH, available on http://www.srjis.com/srjis_new/images/articles/35Dr.PARDEEP%20MITTAL1%20AMANDEEP%20SINGH2.pdf last visited on dated 02.10.2014 at about 2.35 P.M

[2] Cyber Laws in India, available on http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf last visited on dated 02.10.2014 at about 2.18 P.M

one's mobile will tantamount to dumping one in solitary confinement![3]

1.2 What is a Cyber Crime?[4]

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web. There isn't really a fixed definition for cyber crime. The Indian Law has not given any definition to the term 'cyber crime'. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law. But "Cyber Security" is defined under Section (2) (b) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

1.3 What is Cyber Law?[5]

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less of a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a separate chapter XI entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

2. THE VARIOUS KINDS OF CYBER CRIMES[6]

Cyber crimes involve a modification of a conventional crime by using computers. Following is a comprehensive list of the

[3] Id.

[4] Types of Cyber Crimes & Cyber Law in India, available on http://www.csi-india.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6 last visited on dated 02.10.2014 at about 2.16 P.M

[5] Ibid.

[6] CYBER CRIMES AND EFFECTIVENESS OF LAWS IN INDIA TO CONTROL THEM, January 2009, From the SelectedWorks of Mubashshir Sarshar, available on http://works.bepress.com/cgi/viewcontent.cgi?article=1013&context=mubashshir last visited on dated 02.10.2014 at about 2.31 P.M

various types of Crimes which have been committed in the recent times.[7]

a) Hacking

"Hacking" means unauthorized access to a computer system. 13 It is the most common type of Cyber crime being committed across the world. The word „hacking" has been defined in section 66 of the Information Technology Act, 2000 as follows, "whoever with the intent to cause or knowingly that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking" Punishment for hacking under the above mentioned section is imprisonment for three years or fine which may extend up to two lakh rupees or both.

b) Virus, Trojans and Worms

A computer virus is a programme designed to replicate and spread, generally with the victim being oblivious to its existence. Computer viruses spread by attaching themselves to programme like word-processors or spreadsheets or they attach themselves to the boot sector of a disk. Thus when an infected file is activated, the virus itself is also executed. Trojan horse is defined a "malicious, security-breaking program that is disguised as something benign" such as a directory lister, archiver, game, or a programme to search or destroy viruses. A computer worm is a self contained program that is able to spread functional copies of itself or its segments to other computer systems. Unlike viruses, worms do not need to attach themselves to a host program.

c) Cyber Pornography

The growth of technology has flip side to it causing multiple problems in everyday life. The Internet has provided a medium for the facilitation of crimes like pornography. Cyber porn as it is popularly known is widespread. Almost 50 % of the websites exhibit pornographic material today. Pornographic materials can also be reproduced more quickly and cheaply on new media like hard disks and cd-roms. The new technology is not merely limited to texts and images but have full motion video clips and movies too. These have serious consequences and have result in serious offences which have universal disapproval like child pornography which are far easier for offenders to hide and propagate through the medium of the internet.

[7] Id.

d) Cyber Stalking

Cyber stalking can be defined as the repeated acts harassment or threatening behaviour of the cyber criminal towards the victim by using the internet services. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker. Cyber Stalking is a problem which many people especially young teenage girls complain about.

e) Cyber Terrorism

Cyber terrorism may be defined to be "the premeditated use of distruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideologic al, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives". The role of computer with respect to terrorism is that a modern thief can steal more with a computer than with a gun and a future terrorist may be able to cause more damage with a keyboard than with a bomb. No doubt, the great fears are combined in terrorism, the fear of random, violent, victamisation segues well with the distrust and out of fear of computer technology. Technology is complex, abstract and indirect in its impact on individual and it is easy to distrust that which one is not able to control. People believe that technology has the ability to become the master and humanity its servant.

f) Cyber Crime Related to Finance

There are various types of Cyber Crimes which are directly related to financial or monetory gains by illegal means. To achieve this end, the persons on the cyber world who could be suitably called as fraudsters uses different techniques and schemes to befool other people on the internet. Online fraud and cheating is one the most lucrative businesses that are growing today in the cyberspace. It may assume different forms. Some of the cases of online fraud and cheating have come to light are pertaining to credit-card crimes, contractual crimes, online auction frauds, online investment schemes, job offerings, etc.

g) Cyber Crimes Involving Mobile and Wireless Technology

At present the mobile technology has developed so much that is becomes somewhat equivalent to a personal computer. There is also increase in the services which were never available on mobile phones before, such as mobile banking, which is also prone to cyber

crimes. Due to the development in the wireless technology the cyber crimes on the mobile device is coming at par with the cyber crimes on the net day by day.

h) Phishing

In computing, phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit cards, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to a "fish" for users" financial information and passwords. The act of sending an email to a user falsely claiming to be an established and legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

i) Denial of Service Attacks (Dos Attack)

This is an act by a criminal who floods the bandwidth of the victim's network or fills his email box with spam mail depriving him of the service he is entitled to access or provide Short for denial-of-service attack, a type of service attack on a network which is designed to bring the network down to its knees by flooding it with useless traffic. Many DoS attack such as Ping of Death and Teardrop attack, exploit limitation in the TCP/IP protocols. For all known DoS attacks, there are softwares fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by hackers. This involves flooding computer resources with more requests than it can handle.

j) Email Bombing

In internet usage, an email-bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox. Mail bombing is the act of sending an email bomb, a term shared with the act of sending actual exploding devices. There are two ways of e-mail bombing, mass mailing and list linking. Mass mailing consists of sending numerous duplicate mails to the same email ID. These types of mail bombers are simple to design, but due to their extreme simplicity they can be easily filtered by sham filters. List linking on the other hand, consists of signing a particular email ID up to several subscriptions. This type of bombing is effective as the person has to unsubscribe

from all he services manually. In order to prevent this type of bombing most type of services send a confirmation to the mailbox when we register for the subscription on a particular website. E-mail spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users. E-mail spamming can be made worse of the recipients reply to the email, causing all the original addresses to receive the reply.

k) Email Spoofing

E-mail spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used for spam email and phishing to hide the origin of an email message. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields, ill intentioned users can make the email appear to be from someone other than the actual sender. It is often associated with website spoofing which mimic an actual well-known website but are run by other party either with fraudulent intentions or as a means of criticism of the organization's activities.

l) Data Diddling

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, or a virus that changes data, or the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved the process of creating, recording, encoding, examining, checking, converting or transmitting data.36 This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

m) Salami Attacks

A salami attack is a series of minor data-security attack that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can be considered a Salami Attack. Crimes involving salami attacks are typically difficult to detect and trace. These attack are used for commission of financial crimes. These key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program into the bank servers that

deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount each month.

n) Logic Bombs

A logic bomb is a programming code, inserted surreptitiously or intentionally and which is designed to execute under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. Software that is inherently malicious, such as viruses and worms, often contains logic bombs that execute a certain payload at the pre-defined time or when some other conditions are met. Many viruses attack their hosts systems on specific days, e.g. Friday the 13th and April fool's day logic bombs. A logic bomb when exploded may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.

o) Internet Time Theft

Theft of Internet hours refers to using someone else's internet hours. Secion 43 (h) of the IT Act, 2000 lays down civil liability for this offence. It reads as, whosoever without the permission of the owner or any other person who is in charge a computer system or computer network, charges the service availed of by a person to the account of another person by tampering with or manipulating any computer, computer systems or network is liable to pay damages not exceeding one crore to the person in office.

p) Web Jacking

This term is derived from the term hi jacking. This occurs when someone forcefully takes control of a website by cracking the password and then changing it. The actual owner of the website does not have any control over what appears on that website.

3. POSITIVE & NEGATIVE ASPECTS OF IT ACT, 2000

Information Technology Act, 2000 deals with the cyber crime problems. It has some positive as well as negative aspects.[8]

3.1 Positive Aspects of the IT Act, 2000[9]

[8] Cyber Crimes & Cyber Law - the Indian perspective, available on http://www.legalserviceindia.com/article/l323-Cyber-Crimes-&-Cyber-Law.html last visited on dated 02.10.2014 at about 2.28 P.M

[9] Id.

a) Prior to the enactment of the IT Act, 2000 even an e-mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the IT Act, 2000 changed this scenario by legal recognition of the electronic format. Indeed, the IT Act, 2000 is a step forward.

b) From the perspective of the corporate sector, companies shall be able to carry out electronic commerce using the legal infrastructure provided by the IT Act, 2000. Till the coming into effect of the Indian Cyber law, the growth of electronic commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.

c) Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the IT Act, 2000.

d) In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a back up. Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy if any one breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the IT Act, 2000 is in the form of monetary damages, by the way of compensation, not exceeding Rs. 1, 00, 00,000.

e) IT Act, 2000 has defined various cyber crimes which includes hacking and damage to the computer code. Prior to the coming into effect of the Indian Cyber law, the corporate were helpless as there was no legal redress for such issues. But the IT Act, 2000 changes the scene altogether.

3.2 The Grey Areas of the IT Act, 2000[10]

a) The IT Act, 2000 is likely to cause a conflict of jurisdiction.

b) Electronic commerce is based on the system of domain names. The IT Act, 2000 does not even touch the issues relating to domain names.

[10] Ibid.

Even domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law.

c) The IT Act, 2000 does not deal with any issues concerning the protection of Intellectual Property Rights I the context of the online environment. Contentious yet very important issues concerning online copyrights, trademarks and patents have been left untouched by the law, thereby leaving many loopholes.

d) As the cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defined in the IT Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. The IT Act, 2000 does not cove various kinds of cyber crimes and Internet related crimes. These Include:

- Theft of Internet hours
- Cyber theft
- Cyber stalking
- Cyber harassment
- Cyber defamation
- Cyber fraud
- Misuse of credit card numbers
- Chat room abuse

e) The IT Act, 2000 has not tackled several vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few. Privacy issues have not been touched at all.

f) Another grey area of the IT Act is that the same does not touch upon any anti- trust issues.

g) The most serious concern about the Indian Cyber law relates to its implementation. The IT Act, 2000 does not lay down parameters for its implementation. Also, when internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian cyber law raises more questions than it answers.

4. CYBER CRIMES- INDIAN CASES[11]

[11] CYBER CRIMES: LAW AND PRACTICE available on

a) Pune Citibank Mphasis Call Center Fraud

It is a case of sourcing engineering. US $ 3,50,000 from City bank accounts of four US customers were dishonestly transferred to bogus accounts in Pune, through internet. Some employees of a call centre gained the confidence of the US customers and obtained their PIN numbers under the guise of helping the customers out of difficult situations.. Later they used these numbers to commit fraud. Highest security prevails in the call centers in India as they know that they will lose their business. The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

b) State of Tamil Nadu Vs Suhas Katti

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the *yahoo message group*. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits. The court relied upon the expert witnesses and other evidence

---

http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf last visited on dated 02.10.2014 at about 2.17 P.M, cf. http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf

produced before it, including witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved and convicted the accused. This is considered as the first case in Tamil Nadu, in which the offender was convicted under section 67 of Information Technology Act 2000 in India.

c) The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

d) SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra

In this case, the defendant Jogesh Kwatra being an employee of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from sending derogatory emails to the plaintiff. The plaintiff contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature and the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world.

The Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs. This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an injunction

restraining the defendant from defaming the plaintiffs by sending defamatory emails.

e) Parliament Attack Case

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analyzing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD. The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

f) Andhra Pradesh Tax Case

The owner of a plastics firm in Andhra Pradesh was arrested and Rs. 22 crore cash was recovered from his house by the Vigilance Department. They sought an explanation from him regarding the unaccounted cash. The accused person submitted 6,000 vouchers to prove the legitimacy of trade, but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It was revealed that the accused was running five businesses under the guise of one company and used fake and computerized vouchers to show sales records and save tax. Thus the dubious tactics of the prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person.

5. RECOMMENDATIONS FOR PROTECTION AGAINST CYBER CRIMES[12]

a) Firms should secure their networked information

Laws to enforce property rights work only when property owners take reasonable

[12] Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information, December 2000, available on http://www.witsa.org/papers/McConnell-cybercrime.pdf last visited on dated 02.10.2014 at about 2.28 P.M

steps to protect their property in the first place. As one observer has noted, if homeowners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police? Even where laws are adequate, firms dependent on the network must make their own information and systems secure. And where enforceable laws are months or years away, as in most countries, this responsibility is even more significant.

b) Governments should assure that their laws apply to cyber crimes

National governments remain the dominant authority for regulating criminal behavior in most places in the world. One nation already has struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by cyber crime. It is crucial that other nations profit from this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals. In many cases, nations will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat.

c) Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security

To be prosecuted across a border, an act must be a crime in each jurisdiction. Thus, while local legal traditions must be respected, nations must define cyber crimes in a similar manner. An important effort to craft a model approach is underway in the Council of Europe comprising 41 countries. The Council is crafting an international Convention on Cyber Crime. The Convention addresses illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes. It also addresses investigational matters related to jurisdiction, extradition, the interception of communications, and the production and preservation of data. Finally, it promotes cooperation among law enforcement officials across national borders.

6. CONCLUSION

Society[13] as on today is happening more and more dependent upon technology and crime based on electronic offences are bound to increase. Endeavor of law making machinery of the nation should be in accordance with mile compared to the fraudsters, to keep the crimes lowest. Hence, it should be the persistent efforts of rulers and law makers to ensure that governing laws of technology contains every aspect and issues of cyber crime and further grow in continuous and healthy manner to keep constant vigil and check over the related crimes.

[13] India: An Overview Of Cyber Laws vs. Cyber Crimes: In Indian Perspective, Article by Rohit K. Gupta, Singh & Associates, available on http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective last visited on dated 02.10.2014 at about 2.14 P.M