MOBILE TECHNOLOGY AND CRIME RELATED TO IT

What is mobile technology and what are the benefits?

Mobile technology is exactly what the name implies – technology that is portable. Mobile IT devices include:

- Laptop computers.
- Palmtop computers or personal digital assistants.
- Mobile phones and 'smart phones' – high-end phones with more advanced capabilities.
- Global positioning system (GPS) devices.
- Wireless debit/credit card payment terminals.

Mobile devices can be enabled to use a variety of communications technologies such as;

- Wireless fidelity (WiFi) – a type of wireless local area network technology.
- Bluetooth – connects mobile devices wirelessly.
- 'Third Generation' (3G), global system for mobile communications (GSM) and general packet radio service (GPRS0 data services – data networking services for mobile phones.
- Dial-up-service – data networking services using modems and telephone lines.
- Virtual private networks – secure access to a private network.

It is therefore possible to network the mobile device to a home office or the internet while travelling.

Benefits

- Mobile computing can improve the service you offer your customers. For example, you could use your laptop computers to give a presentation. Or you could remotely to your diary to arrange a follow-up appointment.
- More powerful solutions can link you directly into the office network while working off site, for instance to access your company's database or accounting systems.
- This leads to great flexibility in working – for example, enabling home working, or working while travelling. Increasingly, networking 'hot spots' are being provided in public areas that allow connection back to the office network or the internet.

Drawbacks

- Mobile IT devices can expose valuable data to unauthorized people if proper precautions are not taken to ensure that the devices, and the data they can access, are kept safe.

ARE CYBER CRIME AND MOBILE CRIME SAME?

In today's world with the advent of SMART PHONES there is virtually no difference between COMPUTER and MOBILE phones, so whatever Cyber Crime we were aware of related to Computers are also applicable to Mobile Crime.

What is Cyber Crime? – A definition.

Defining cyber crimes, as "acts that are punishable by the Information technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending threatening emails etc. a simple yet sturdy definition of cyber crime would be "unlawful acts wherein computer is either a tool or a target or both.

Criminals can operate anonymously over the computer networks, hackers invade privacy, hackers destroy "Property" in the form of computer files or Records.

- Hackers Injure Other Computer Users by Destroying Information System.
- Computer Pirates Steal Intellectual Property.

CRIME RALATED TO THE MOBILE TECHNOLOGY

- As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is nor necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with criminal element. According to Donn Parker, "For the first time in human history, computers and automated processes make it possible to possess, not just commit, a crime. Today, criminals can pass a complete crime in software from one to another, each improving or adapting it to his or her own needs."
- The first recorded cyber crime took place in the year 1820. The era of modern computers, however, began with the analytical engine of Charles Babbage. Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber crime has assumed rather threatening implications.
- The majority of what are termed "cyber crimes" is really violations of longstanding criminal law, perpetrated through the use of computers or information networks. The problems of crime using

computers will rarely require the creation of new substantive criminal law; rather, they suggest need for better and more effective means of international co-operation to enforce existing laws.

- On the other hand, there are new and serious problems posed by attacks against computer and information systems, such as malicious hacking, dissemination of viruses, and denial-of-service attacks. Such attacks should be effectively prohibited, wherever they may originate. At the same time, it is to be remembered that often the most effective way to counter such as attacks is to quickly deploy technical countermeasures; therefore, to the extent that well-meaning but overbroad criminal regulations diminish the technical edge of legitimate information security research and engineering, they could have the unintended consequences of actually undermining information security.

Classification of Cyber Crimes

The Information Technology Act deals with the following cyber crimes along with others

- Tampering with computer source documents
- Hacking
- Publishing of information, which is obscene in electronic form
- Child Pornography
- Accessing protected system
- Breach of confidentiality and privacy

TYPES OF CYBER/MOBILE CRIME

Cyber crime other than those mentioned under the IT Act

- Cyber Stalking
- Cyber squatting
- Data Diddling
- Cyber Defamation
- Trojan Attack
- Forgery
- Financial crimes
- Internet time theft
- Virus/worm attack
- E-mail spoofing
- E-mail bombing
- Salami attack
- Web jacking

Cyber/Mobile Criminals

- Any person who commits an illegal act with a guilty intention or commits a crime is called an offender or a criminal. In this context, any person who commits a Cyber Crime is known as a Cyber Criminal. The Cyber Criminals may be children and adolescents aged between 6 to 18 years. They may be organized hackers, may be professional hackers or crackers, discontented employees, cheaters or even psychic person.

A. Kids & Teenagers (age group 9 – 16 etc)

- This is really difficult to believe but it is true. Most amateur hackers and cyber crime criminals are teenagers. To them, who have just begun to understand what appears to be a lot about computers, it is a matter of pride to have hacked into a computer system or a website. There is also that little issue of appearing really among friends. These young rebels may also commit cyber crimes without really knowing that they are doing anything wrong.
- According to the BBC, teen hackers have gone from simply trying to make a name for themselves to actually working their way into a life of crime from the computer angle. According to Kevin Hogan, one of the biggest changes of 2004 was the waning influence of the boy hackers play around with malicious code, 2004 saw a significant rise in criminal use of malicious programs. The financial incentives were driving criminal use of technology.
- Another reason for the increase in number of teenage offenders in cyber crimes are that many of the offenders who are mainly young college students are unaware of its seriousness. Recently the Chennai city police have arrested an engineering college student from Tamil Nadu for sending unsolicited message to a chartered accountant. The boy is now released on bail. So counseling session for college students has to be launched to educate them on the gravity and consequences emanating from such crimes.
- In September, 2005, A Massachusetts teenager pleaded guilty in federal court in Boston for a string of hacking crimes reported to include the February compromise of online information broker Lexis Nexis and socialite Paris Hilton's T-Mobile cellular phone account. The US Court noted that the number of teenage hackers is on the rise and only the lowest 1 percent of hackers is caught.

B. Organized hacktivists

- Hacktivists are hackers with a particular (mostly political) motive. In other cases this reason can be social activism, religious activism, etc. The attacks on approximately 200 prominent Indian websites

by a group of hackers known as Paskistani Cyber Warriors are a good example of political hactivists at work.

C. Disgruntled employees

- One can hardly believe how spiteful displeased employees can become. Till now they had the option of going on strike against their bosses. Now, with the increase independence on computers and the automation of processes, it is easier for disgruntled employees to do more harm to their employers by committing computer related crimes, which can bring entire systems down.

D. Professional hackers (Corporate espionage)

- Extensive computerization has resulted in business organizations storing all their information in electronic form. Rival organizations employ hackers to steal industrial secrets and other information that could be beneficial to them. The temptation to use professional hackers for industrial espionage also stems from the fact that physical presence required to gain access to important documents is rendered needles if hacking can retrieve those.

Criminal Law – General Principles

- According to law, certain persons are excluded from criminal liability for their actions, if at the relevant time; they had not reached an age of criminal responsibility. After reaching the initial age, there may be levels of responsibility dictated by age and the type of offense allegedly committed.
- Governments enact laws to label certain types of activity as wrongful or illegal. Behavior of a more antisocial nature can be stigmatized in a more positive way to show society's disapproval through the use of the word criminal. In this context, laws tend to use the phrase, "age of criminal responsibility" in two different ways:
    1. As a definition of the process for dealing with alleged offenders, the range of ages specifies the exemption of a child from the adult system of prosecution and punishment. Most states develop special juvenile justice systems in parallel to the adult criminal justice system. Children are diverted into this system when they have committed what would have been an offense in an adult.
    2. As the physical capacity of the child to commit a crime. Hence, children are deemed incapable of committing some sexual or other acts requiring abilities of a more mature quality.
- The age of majority is the threshold of adulthood as it is conceptualized in the law. It is the chronological moment when children legally assume majority control over their actions and decisions, thereby terminating the legal control and legal responsibilities of their parents over and for them. Bu in the cyber world it is not possible to follow these traditional principles of criminal law to fix liability. Statistics reveal that in cyber crime world, most of the offenders are those who are under the age of majority. Therefore, some other mechanism has to be evolved to deal with cyber criminals.
- Ethics and morality in different circumstances connotes varied and complex meaning. Each and everything which is opposed to public policy, against public welfare and which may disturb public tranquility may e immoral and unethical.
- In the past terms such as imperialism, colonialism, apartheid, which were burning issues have given way to cyber crime, hacking, 'cyber-ethics' etc. Today in the present there is a need to evolve a 'cyber-jurisprudence' based on which 'cyber-ethics' can be evaluated and criticized. Further there is a dire need for evolving a code of Ethics on the Cyber-Space and discipline.
- The Information Technology Act 2000 was passed when the country was facing problem of growing cyber crimes. Since the Internet is the medium for huge information and a large base of communications around the world, it is necessary to take certain precautions while operating it. Therefore, in order to prevent cyber crime it is important to educate everyone and practice safe computing.

IS INDIAN LAW SUFFICIENT TO HANDLE MOBILE CRIME?

- The problem of data theft which has emerged as one of the major cyber crimes worldwide has attracted little attention of law makers in India. Unlike U.K which has The Data protection Act, 1984 there is no specific legislation in India to tackle this problem, though India boasts of its Information technology Act, 2000 to address the ever growing menace of cyber crimes, including data theft. The truth is that our IT Act, 2000 is not well equipped to tackle such crimes. The various provisions of the IT Act, 2000 which deals with the problem to some extent are briefly discussed below.
- **Section 43:-** This section provides protection against destruction and unauthorized access of the computer system by imposing heavy penalty up to one crore. The unauthorized downloading extraction and copying of data are also covered under this section. Clause 'C' of this section impose penalty for unauthorized introduction of computer viruses of contaminants. Clause 'G' provides penalties for assisting the unauthorized access.
- **Section 65:-** This section provides for computer source code. If anyone knowingly or intentionally conceals, destroys, alters or causes another to do as such shall have to suffer imprisonment of up to 3 years or fine up to 2 lakh rupee. Thus protection has been provided against tampering of computer source documents.
- **Section 66:-** Protection against hacking has been provided under this section. As per this section, hacking is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss or damage will be caused to any person an information residing in a

computer resource must be either destroyed, deleted, altered or its value and utility get diminished. This section imposes the penalty of imprisonment of up to three years or fine up to 2 lakh rupee or both on the hacker.

- **Section 70:-** This section provides protection of the data stored in the protected system. Protected systems are those computers, computer system or computer network to which the appropriate government, by issuing gazette information in the official gazette, declared it as protected system. Any access or attempt to secure access of that system in contravention of the provision of this section will make the person accessed liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine.
- **Section 72:-** This section provides protection against breach of confidentiality and privacy of the data. As per this, any person upon whom powers have been conferred under IT Act and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupee or both.

Can Data theft be covered under IPC?

- ***Section 378 of the Indian Penal Code, 1860 defines 'Theft' as follows:-***
  Theft – Whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.
- **Section 22 of IPC, 1860 defines "movable property" as follows**
  "The words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth."
- Since section 378 IPC, only refers to "Movable Property" i.e. Corporeal Property, and Data by itself is intangible, it is not covered under the definition "Theft". However, if Data is stored in a medium (CD, Floppy etc.) and such medium is stolen, it would be covered under the definition of 'Theft', since the medium id\s a movable property. But, if Data is transmitted electronically, i.e. in intangible form, it would not specifically constitute theft under the IPC.
- "Data", in its intangible form, can at best be put at par with electricity. The question whether electricity could be stolen, arose before Hon'ble Supreme Court in the case "Avtar Singh vs. State of Punjab" (AIR 1965 SC 666). Answering the question, the Supreme Court held that electricity is not a movable property, hence, is not covered under the definition of "Theft" under section 378 IPC. However, since section 39 of the Electricity Act extended Section 378 IPC to apply to electricity, so it became specifically covered within the meaning of "theft:. It is therefore imperative that a provision like in the Electricity Act be inserted in the IT Act, 2000 to extend the application of section 378 IPC to data theft specifically.

What do we need and why do we need?

- It is imperative in today's worlds that an emerging IT super power like India has a comprehensive legislation to protect its booming IT and BPO Industries (worst affected industries) against such crimes. Though the IT Act may appear sufficient in this regard but it is not comprehensive enough to tackle the minute technological intricacies involves in such a crime which leaves loopholes in the law and culprits get away easily. Since this problem is not confirmed to one nation and has international dimensions, India must look forward to be a signatory to any international convention or treaty in this regard. Also if high time that our national police organizations are trained to deal with such crimes.

SIM CLONING

SIM (*Subscriber Identity Module*) cloning is the latest phenomena and potentially, in financial terms, may go well beyond the multi-million pounds mobile telephone cloning industry. So what is SIM cloning?
The abstract conceptualization of cloning comprehended by most people is that of "duplication" of original information and so it may appear patronizing and rather trite for this article to start extrapolating a semantic view of the word 'cloning'. It is relevant to briefly review the issue of cloning in context with GSM SIMs. In April, 1988 the Smartcard Developers Association (SDA) and two U.C.Berkeley researchers jointly announced, following examination of GSM security for SIM, the discovery, after a day's examination, of a fatal cryptographic flaw in COMP128, the algorithm used to protect the identity inside the SIM. In order to protect the identity the SIM needs to keep its secret authentication key (Ki) secure.

- The release of the security flaw discovery into the public domain generated reports in the various media, all around the world. Industry responded to ally fears and reassure users with respect to GSM's authentication security. One proposition mooted was that the time and expense it would take to clone just one SIM made it likely to see a spawning of cloning factories.