B.A.LL.B. VIII Semester

Paper Code: 403

Subject: Law and Technology

SYLLABUS

Unit – I: E-COMMERCE

a. Online contracting

b. Online securities offering

c. E-Banking

Unit – II: Cyber Crimes

a. Obscenity

b. Defamation

c. Hacking and Cracking

d. Crime through Mobile Phones

Unit – III: Genetic and Medical Technologies

a. Regulation of Genetic Technology

b. Laws on Medical Technology

Unit –IV: Broadcasting

a. Regulation and Control of Broadcasting

b. Law relating to Cable Television Network

UNIT-I

E-COMMERCE

A. ONLINE CONTRACTING

A "cyber" or electronic contract is a contract created wholly or in part through communications over computer networks. A cyber-contract can be created entirely by the exchange of e-mails where an offer and an acceptance are evident or they can be made by a combination of electronic communications, paper documents, faxes and oral discussions.

Electronic contracts can add the element of speed and efficiency to the contracting process but several legal issues must dealt with in the process, as follows:

WHAT ARE THE TERMS OF THE ELECTRONIC CONTRACT?

Frequently parties to a contract do not always clearly address all of the contract terms. Terms may be missing or unclear, or the parties may have exchanged conflicting documents. In these cases, how are the terms of the contract determined?

The general rules of contract law follow a hierarchy of evidence when determining the terms of a vague or incomplete contract, as follows:

a) The terms stated in the discussions and writings exchanged by the parties that are not in conflict;

b)Terms implied by the current and past conduct of the parties;

c)Terms implied by industry custom and practice; and

d) Terms implied by law, i.e., damages for breach, liability for negligence, jurisdiction andvenue, etc.

If a planner and supplier exchange promises by e-mail the law will interpret this agreement the same way it would interpret a more traditional contract written on paper. Parties to an electronic contract should be just a careful in articulating the terms as they would be in traditional contracts.

IMPOSTORS AND PERSONS WITHOUT AUTHORITY

The daily news is full of headlines detailing the latest computer scam causing someone to lose a lot of money. The biggest concern in electronic communication is the identity and authority of the person on the other side of the transaction. It is a simple matter for a person to adopt a

pseudonym on-line or to send an electronic message that appears to come from someone else. This person could be anyone from a curious competitor to a dishonest person with too much time on their hands. It could even be a disgruntled former employee.

For those who want to engage in on-line contracting, two major issues arise: (1) How can you be sure that the person with whom you are communicating is the person he or she claims to be? and (2) Can an impersonator bind you to an electronic contract?

Since electronic communications does not involve business cards, letterhead or corporate seals it is impossible for one party to determine the other party's authority to book a meeting or sign a contract. Just because someone has a corporate e-mail address and says they are the executive director, vice-president of special events or director of meeting planning does not make it so. Parties to an on-line contract must still exercise due diligence to ascertain who they are dealing with on the other side. The development of digital signatures is helping to solve this problem.

Everyone is (or should be) concerned with someone else impersonating them and fraudulently signing their name to contracts. The key issue of course is who, if anyone, is bound to these contracts. Under current law a forged signature will only bind the forger, not the party being impersonated. The other party to the transaction, however, may be left holding an empty bag if the impostor can't be caught or identified or if the impostor is in no position to perform on the fraudulent contract. The exception to this is if the real party ratifies the signature or was somehow negligent and contributed to the forgery. This is just as true in on-line contracts as it is in traditional paper contracts. Again, digital signatures (discussed below) are solving some of these problems however new laws are being proposed that would hold business people liable for not providing an adequate level of security for their digital signatures.

These issues are not unique to on-line communications. Impostors and persons without authority operate in paper transactions as well. The difference is that in on-line communications there is greater anonymity and greater ease in perpetrating fraud without a great deal of financial investment. Technology companies and lawmakers are dealing with these issues daily and the result is new techniques to combat the potential for fraud in on-line communications. As mentioned above, one of these new techniques is the creation of digital signatures (discussed below). A digital signature can provide assurance that the communication was sent by a known party and not an impostor.

LEGAL REQUIREMENTS FOR ELECTRONIC CONTRACTS:

For the business world in general, and the meetings industry specifically, to embrace electronic contracts the exchange and storage of these records must satisfy certain legal requirements. These requirements generally include the following:

a) Authenticity

b) Integrity

c) Nonrepudiation

d) Writing and signature

e) Confidentiality

These requirements are not always present in every situation but they are applicable to most.

AUTHENTICITY

Authenticity is concerned with the source or origin of a communication. Who is the message from? Is it genuine or a forgery? Every party to an electronic contract must have confidence in the authenticity of the messages it receives. A party who fails to verify the other party's identity in any transaction may have no recourse if a fraud is perpetrated. Communications that cannot be authenticated in a tangible form may not be used as evidence in a court room.

INTEGRITY

Integrity is concerned with the accuracy and completeness of the communication. Both senders and receivers of electronic communications must be able to tell: is the message sent identical to the message received?, is the message complete or has something been lost in transmission?, has the message been altered in any way either in transmission or in storage? Messages sent over the Internet pass through many routing stations and packet-switching nodes. Hence, there are many opportunities for messages to be altered along the way to their final destination.

For example, a meeting sponsor needs to know that a supplier's reply to a request for proposal is accurate and can be relied on.

NON-REPUDIATION

Nonrepudiation is concerned with holding the sender to the communication he or she sent. The sender should not be able to deny having sent the communication if he or she did, in fact, send it, or to claim that the contents of the communication as received are not the same as what the sender sent if, in fact, they are what was sent. When a contract is in dispute, the party relying on it must be able to prove that the other side actually agreed to the deal.

WRITING AND SIGNATURE

As a general rule, contracts do not have to be in writing or even signed by either party to be enforceable. Contracts may be formed by conduct of the parties and may be oral unless they fall under the Statute of Frauds. The Statute of Frauds is a series of statutes that have been passed in

most states that require that certain types of contracts must be in writing to be enforceable. In the meetings industry two of the types are prevalent:

a) Contracts that can't be performed in one year from the date they are made, and

b) Contracts for the sale of goods over $500.

When the statute of frauds applies, there must be a writing sufficient to indicate that a contract has been made between the parties. The definition of a writing is not limited to ink on paper. Rather, the essence of the requirement is that the communication be reduced to a tangible form. Electronic transmissions recorded in a tangible form should meet the writing requirement. To ensure this result it is probably necessary to preserve electronic communications, such as e-mails, in printed form or in a computer log.

In many cases, the law requires that an agreement be both in writing and signed by the person who is sought to be held bound in order for that agreement to be enforceable. If two parties are entering into a contract on-line, these writing and signature requirements may apply.

Generally, a signature is "any symbol executed or adopted by a party with present intention to authenticate a writing. Therefore, a signature need not be ink on paper -- rather, the issue is the intent of the signer. A symbol or code on an electronic record, intended as a signature by the signer, should meet the statute of frauds requirement. Digital signatures (discussed below) should certainly do so.

CONFIDENTIALITY

Confidentiality is concerned with controlling the disclosure of information. Corporate meeting planners for instance may not want the general public to know about the content of the upcoming meeting that concerns a new product. Suppliers may not want everyone to know the special rates being quoted to a particular group.

DIGITAL SIGNATURES

Most persons are comfortable with traditional contracts because of the security and familiarity with paper documents and handwritten signatures. In on-line contracts the security factor has been missing in the past and there is not much familiar with electronic lines of type. In other words, it is easy to be a victim of fraud when conducting business entirely on-line.

The technology industry recognized early on the pitfalls inherent in on-line communications. They have risen to the occasion by creating systems and procedures for satisfying the business and legal requirements of authenticity, integrity, nonrepudiation, writing and signature, and confidentiality. The primary tool in use is digital signatures.

A digital signature is an electronic substitute for a manual signature and is generated by a computer rather than a pen. It serves the same functions as a manual signature, and a lot more.

A digital signature is not a replication of a manual or typed signature such as "signed, John Smith". In technical terms, digital signatures are created and verified by a special application that generates cryptographic messages. Cryptography is a branch of applied mathematics and involves transforming clear messages into seemingly unintelligible forms and back again. For digital signatures to work, two different translation keys are generally used. The first, called a public key, creates the digital signature by transforming the data into an unintelligible code. The second key, called a private key, verifies the digital signature and returns the message into its original form.

A person's public key is distributed by the person to other's with whom they do business. One way of accomplishing this is to post the public key on an organization's web page for anyone to access. A public key can also be attached to the document being executed. Individual's using a digital signature will also have a private key that is known only to that individual, or a limited number of corporate officers. The private key is used to create the digital signature. The document's recipient must have the corresponding public key in order to verify that the digital signature is the signer's.

This system is totally secure as long as the private key is kept private. This is because a digital signature is derived from the document itself. Any change to the document will produce a different digital signature.

A digital signature has many advantages over a manual signature. Both are used to signify authorship, acknowledgment and acceptance of terms. A digital signature, however, also serves an important information security purpose that a manual signature cannot. Digital signatures allow the recipient to determine if the digitally signed communication was changed or not after it was digitally signed. This feature provides integrity and authenticity to a communication that a manual signature does not. Additionally, a message sender can include information about the sender's authority and job title as well as the sender's identity encrypted into their digital signature.

HOW ARE DIGITAL SIGNATURES ACTUALLY SIGNED AND THEN VERIFIED?

A sender must first create a public-private key pair before an electronic communication can be digitally signed. As mentioned above, the sender discloses his or her public key to the recipient. The private key is kept confidential by the sender and is used for the purpose of creating a digital signature.

The entire process is started by the sender who runs a computer program that creates a message digest (technically known as a one-way hash value). The program then encrypts the message

digest using the sender's private key. The encrypted message digest is the digital signature. The sender attaches the digital signature to the communication and sends both electronically to the intended recipient.

When the digitally signed communication is received the recipient's computer runs a computer program containing the same cryptographic mathematical formula that the sender used to create the digital signature. The digital signature is automatically decrypted using the sender's public key. If the recipient's program is able to decrypt the digital signature successfully, he or she knows that the communication came from the purported sender. Further, the recipient can tell if a communication has been altered or tampered with because the recipient's program will create a second message digest of the communication. This second message digest is then compared to the original message digest. If the two match the recipient has now verified the integrity of the message. Messages, of course, can be a few sentences long or an entire facility contract.

This system is virtually foolproof as long as the public key used by a sender can be verified as indeed belonging to that sender versus an impostor. This potential risk has been solved by the use of third parties to verify an individual's public key. Such a third party is called a certification authority. Several national companies serve in this capacity for individuals and organizations for a nominal fee.

THE LEGAL EFFECT OF A DIGITAL SIGNATURE

Although the law is still evolving in this area, a number of states have passed statutes authorizing the use of digital signatures and outlining details for their use. Most of the state laws are based on the American Bar Association Guidelines for Digital Signatures.

If the proper guidelines are followed, digital signatures should meet all of the legal requirements for electronic contracts. Digital signatures accomplish the following. They can : 1) provide a means to verify the integrity of messages sent, 2) verify the source of an electronic message because only a sender's public key will decrypt a digital signature encrypted with the sender's private key, 3) prevent repudiation by the sender once the authenticity and integrity of a communication have been established, and 4) satisfy the requirement for a writing and signature required by the Statute of Frauds.

CONCLUSION

Although the meetings industry is still primarily dependent on the use of paper in creating contracts, the full use of electronic or "cyber-contracts" is probably not far away. Such cyber-contracts will not take the place of full scale negotiations but they will definitely speed up the end game of signing contracts once the details are agreed to by the parties. As business and technology race forward, the use of electronic contracts and digital signatures in the future will

probably seem as commonplace as sticking a piece of paper in a fax machine for someone far away to sign does today.

B. ONLINE SECURITIES OFFERING

Copyright is automatically created on original works. You do not need to file to create a copyright. But it may be a good idea to file a copyright to establish a public record of it and if you ever want to pursue an infringement suit, it will need to have been filed. You can visit **copyright.gov/forms** to download a copyright form. A common-law copyright is created automatically on publication, so registration is not required to use the © symbol. The proper way to state that something is copyrighted is to use the © symbol, the copyright or abbreviated version (Copr.), the year of first publication, and the name of the copyright owner. For example: © Copyright 2007 Off the Page Creations.

Copyrights that were created after January 1, 1978 have protection during the life of the author plus 70 years. In the case of more than one author, the period of protection is the term of 70 years after the death of the last surviving member. In a case of 'Work-Made-For-Hire', the protection term is 95 years from first publication or 120 years from the year of creation (whichever comes first). Once copyrights expire they become part of the public domain and are free to use by anyone. But don't assume just because something doesn't have a copyright symbol, that it is free to use.

In a 'Work-Made-For-Hire' the person that hires someone to create (design a logo for example) something for them, the person hiring is the person who holds the copyright, not the designer or author. If the work was prepared by an employee within his job duties as requested by his/her boss and not for a customer, the employer holds the copyright because the employee was hired to do it for the employer and it was part of his/her job duties.

An odd variation to the 'Work-Made-For-Hire' rule is websites (including the 'look & feel', the software, scripts, graphics & the text). If someone hires a web designer to create their website, the website designer holds the copyright, unless it is specified otherwise in the contract. Most companies state that the hiring party holds the contract (as we state in our contract), but it's a good idea to verify who will hold copyright to the website before signing anything.

Fair Use

'Fair Use' allows limited use of a copyrighted work. Some examples of what are considered 'fair use' are: teaching, criticism, comment, news reporting, and research. Only a court can decide if a copyrighted works use was considered 'fair use'.

What You Can't Do

Copy pictures to use on your brochure or website that you found on the internet (even if you put up the copyright line of who holds the copyright, this is considered infringement)

Purchase a license to use a photo on your brochure, then continue to use it on your website, flyers, and postcards unless it is stated in the license

Copy text out of a book or off from a website and use it verbatim

Put music on your website without permission

Post an article without permission, even if it's about you

Use an image by linking to it rather than copying it (This is still copyright infringement)

What You Should Do

Purchase photos to use that are 'copyright free' and follow the license for the uses

Or get permission from the copyright holder to use photos

Purchase 'copyright free' music and follow the license for the uses

Get permission to use articles from the writer & publisher

You should ask permission to link to someone's website

Copyright infringers may face civil liability and also criminal liability for felony copyright infringement if it is willful, and for financial gain, or by reproducing and distributing a large amount.

If you are looking for a **Copyright Attorney**, I recommend Lexero Law Firm.

Brief Overview About Trademarks

A trademark is a word, name, symbol, device, or combination of, used by someone to identify his product. Trademarks arise from 'use' and do not have to be registered to be considered trademarked. There are good reasons to register a trademark though. One reason, like copyrights, it establishes a public record. The second reason is that it needs to be registered in order to file for trademark infringement. It also helps to establish trademark in other countries and to stop imports of infringing foreign goods from entering the country. A trademark is valid indefinitely, but if not maintained it can be lost and fall into public domain. For instance, if a trademark becomes a common phrase, then it will be deemed lost and the trademarked term considered common usage (Aspirin, Allen Wrench, Granola, and Yo-Yo are just a few examples).

Trademark registration begins with the U.S. Patent and Trademark Office (P.T.O.). Registering a trademark can take more than a year after the application is filed. There is an extensive research involved to ensure that a similar trademark does not already exist.

Once the trademark goes through, the ® symbol identifies a trademark as registered with the U.S. P.T.O. The proper way to write this is - "® Registered in the U.S. Patent and Trademark Office", or the abbreviation - "Reg. U.S. Pat. and Tm. Off." If it is not yet officially registered with the P.T.O., the ™ symbol should be used instead.

Trademarks are protected from infringement and also dilution. Infringement of a trademark means that there is another that is too similar and it is confusing. Dilution of a mark would be because the public has a strong association with the original trademark and the other would take away from that association.

It is not considered infringement to make fun of a copyrighted or trademarked work as long as it is apparent that it is not the original, but a parody. You can not create a domain name similar to another and make fun of it, because it would not be evident that it was a joke until the user actually reached the website.

Trademarks should not be used in meta-tags (the hidden keyword tags on a web page), or in a pay-per click ad campaign. There have been cases where this was considered infringement.

If you are looking for a **Trademark Attorney**, I recommend Lexero Law Firm.

Domain Name Issues

Typosquatting - where a person registers a domain name similar to a real domain name, but with a typo, in hopes that web surfers reach it by accident. These sites are usually filled with paid advertising links that generate revenue for the typosquatter, not to mention the web surfer has been tricked into believing he is on the correct site. This diverts traffic away from the intended site. Sometimes they are routed to a competitors site or a pornographic site.

Cybersquatting - is when someone registers a domain name, in bad faith, violating the rights of the trademark owner. They usually intend to extort payment from the trademark owner, and they keep the names to sell later to the highest bidder.

Pagejacking is when the offender copies part of an existing website, and then puts it up on a different website to make it look like the original. Pagejacking is used in phishing schemes, where the fake page gathers account numbers, passwords, and personal information from the unsuspecting user.

The Uniform Domain Name Dispute Resolution Policy (UDRP) is a cost-effective and faster alternative to a lawsuit, when there is a domain name dispute that needs to be resolved. This was

set up by the Internet Corporation for Assigned Names and Numbers (ICANN), the group responsible for domain name registration.

If you are looking for a **Domain Name Attorney**, I recommend Lexero Law Firm.

SPAM - and how to avoid it

Spam is accounted for around 80% of all U.S. email. 20% of U.S. residents actually buy products from spammers, and this makes it worthwhile for them to continue to harass us with unsolicited emails. There are no laws to prohibit spamming, but there are laws to regulate spam. There are also laws that prevent email harvesting (programs that read through websites looking for email address to add to their database). Many states require opt-in or opt-out options in the email. There are laws that prohibit false headings and laws against spammers that identify their message as coming from someone else. Trademark and unfair competition laws have been used against a spammer whos message reads that it is coming from someone else, and in one case a man was sentenced to 3 years in prison and $16 million in fines. Unfortunately it is very difficult to enforce the statewide spam laws because a sender really has no way of knowing all the states he is sending his spam to by the list of email addresses he has.

There are some things you can do to limit the spam you are getting.

Do Not Reply to Spam! Most times it just confirms they have reached a valid email address and they'll continue to send junk to you.

Do not post your email address on your website - use a form that doesn't display the email, or turn the email address into an image rather then displayed as text.

Use a different email address if you must use one in news groups or forums

Read Terms of Use and Privacy Statements. Don't randomly give out your email address unless you know how it will be used.

Use a spam filter

Never, ever buy from a spammer - this encourages them

Cyber Crimes

Email Spoofing is changing the email header so it looks like its coming from someone else. This is sadly easy to do. This is also used to try to trick people into giving out personal information. This is illegal under the CAN-SPAM Act.

Phishing is a scam where an official-looking email is sent to an unsuspecting user to try to trick them out of their username, password, or other information. They are usually directed to click

onto a link that goes to a fake (spoofed) version of a real organizations website. This is called **Pagejacking**. The address bar can even be altered so it appears to be the official website. If you ever get an email requesting that you verify information by clicking on a link, you should instead **GO DIRECTLY TO THEIR WEBSITE WITHOUT CLICKING ON THE LINK**, to verify it. Lately phishing is even occurring in instant message programs that appear to be coming from a friends IM signature. Always be cautious in this situation.

Vishing is short for 'Voice phishing' and is the latest scam. It may start with an email or it may start with a phone call. These calls can be very believable because often the caller already has your credit card number and just needs you to verify the 3 digit security code on the back of your card. Or it could be an automated system asking you to type in your credit card or account number to verify who you are, which sounds realistic enough.

Keystroke Phishing is when a Trojan program is unknowingly downloaded onto your computer that tracks the keystrokes you enter into the computer, and sends it back to the scammer, who hopes to get a username and password from it.

Identity Theft is where a person gathers your personal information and poses as you to get credit, merchandise, services, or to use the identity to commit other crimes. They obtain this personal information by phishing, database cracking, or survey. Survey is seemingly innocent questions about mother's maiden name, children and pet names, and birth dates that can give access to a surprising amount of passwords and usernames. Once a phisher has your credit card number it can be sold to someone who then creates a credit card to use on an ATM machine. Identity theft is spreading on the internet, but surprisingly it is still **safer to give out your credit card number on the internet then to give it to an unknown salesperson or waiter**. 97% of all identity theft crimes are caused from offline instances, not online. For instance, two places that **identity thieves get your information from are your mailbox, and your trash can**.

<u>Protect Yourself from Identity Theft</u>

Cross-shed documents

Review your credit report twice a year

Be aware of **billing cycles and put vacation holds on mail**

Never reveal your Social Security number unless absolutely necessary

Don't carry seldom used credit cards or unnecessary id's

Be aware that **identity stealers are not always strangers**

Don't give out personal information over the phone, mail or posts on the internet

Take out the hard drive from a computer and destroy it before discarding.**Even if deleted, personal information can still be recovered from a computer's hard drive**

Cookie Poisoning is the modification of cookies that are put on your computer by an attacker to gain information about a user.

Spyware is software that is downloaded onto a user's computer without his knowledge and used for malevolent purposes. It can be downloaded simply by going to a website (called **Drive-by Downloads**), or it can be downloaded unknowingly while installing another program. Spyware can crash computers, slow performance, track emails and visited websites, and track keystrokes that capture the users personal information. Programs such as Spybot, Spy Sweeper, and Ad-Aware can be good for checking and removing these unwanted harmful programs from your computer.

Malware is the malicious software that is developed for the purpose of doing harm. Malware examples are Computer Viruses, Worms, and Trojan horses. A **Worm** is a self-replicating virus that continues to duplicate itself taking up memory and resources. A **Trojan horse** is a hidden program that later gains control and causes damage to your computer.

Wardriving is the practice of driving around in a vehicle with a Wi-Fi enabled laptop looking for available signals to use. War driving steals internet access and is considered a crime of telecommunications theft. Wireless signals can be transmitted 500 feet or more and should be protected with passwords.

Pod Slurping is stealing data by use of iPods, or downloading malicious software via iPods.

Cyberstalking is a crime where the attacker harasses the victim using electronic communication such as email, IM's, chat rooms, discussion groups. Cyber stalkers rely on the anonymity of the Internet thinking they cannot be caught. This may continue to actual physical stalking. Federal law imposes a $1,000 fine or 5 years imprisonment for anyone transmitting in interstate commerce a threat to injure or kidnap someone.

If you are looking for a **Cyber Crime Attorney**, I recommend Lexero Law Firm.

Federal Statutes

Securities Fraud is where someone uses the internet message boards to hype up a stock to drive up the market so he can then sell and make money. It's called the 'Pump and Dump' scheme and is illegal under federal and state laws.

The Fair Housing Act states that you can not discriminate on the basis of race, gender, family status, religion, and national origin. Now that there are many internet postings for rentals by third parties, the question is being raised if the same rules apply to internet postings and who should

be held responsible. The safe harbor provisions of §230 have protected these types of websites from libel or copyright infringement liability provided they remove offending posts when they are notified of the posts. The few times it has been brought up, it was settled out of court and it was agreed to comply with the Fair Housing Act Policy and remove the offending posts.

The USA PATRIOT Act was enacted in response to the September 11th attack in 2001. This act allows electronic messages to be intercepted if it is believed to be of terrorist or criminal activity. It also allows for the retrieval of Internet Service Providers information without going through a court order.

Online Gambling is prohibited or regulated in most states. Many gambling websites originate outside of the country though, and are impossible to shut down. The big worry with online gambling is that minors have access and it enables the pathological gamblers. To try to control this spreading problem, the Unlawful Internet Gambling Enforcement Act was signed into law and makes it illegal for credit card companies, online payment systems, and banks to process payment to online gambling companies. There have also been instances where online casinos and gambling websites owners have been caught in the U.S. and charged with racketeering and mail fraud.

Free Speech and the Internet

The first amendment to the U.S. Constitution guarantees the right to free speech. But there are instances when that can provoke a lawsuit. The four main causes of action against speech on the internet is:

Defamation: "A published intentional false communication that injures a person or company's reputation"

Breach of Contract: If an employee signs a confidentiality agreement and then posts information about products, sales, management, other employees, or rumors, than he may have breached his confidence and trust to the company and be held in Breach of Contract.

Tortious Interference with Business: To file tortious interference there must be an existing contract or business relationship, intentional interference between the company and the business relationship, an effect caused by the action, and damage as a result to the action

Securities Fraud: Attempts to manipulate the price of stock by giving false information or talking it up, so that the stock price goes up, and then selling it (Pump and Dump Schemes), is illegal

If you are looking for a **Free Speech Attorney**, I recommend Lexero Law Firm.

Children and the Internet

The Child Online Protection Act (COPA) makes it a crime to publish "any communication for commercial purposes that includes sexual material that is harmful to minors, without restricting access to such material by minors."

Online Harrassment

When a harasser uses the internet to cause substantial emotional distress to his or her victim, this is considered Online Harrassment. It can take the form of email, chat rooms, instant messaging, newsgroup posts, or message board posts. The largest amount of online harrassment occurs by teenagers who often do not yet understand the impact of their actions and are not yet able to control their emotions.

Online harassment is a crime in some states. If you are harrassed online, you should archive the conversation and report them to the ISP and local law enforcement.

Blogs

When writing in a blog or posting to a message board, keep in mind that you can not write things about people that are not true. You can write something bad about a person, but you can't write something that is untrue and may affect his or her reputation. Truth is a defense to a charge of libel (written) or slander (spoken), if it can be proven true.

Blogs can feel like a personal diary, but one should keep in mind when writing in it, that it's not just a way to vent feelings. The world can read it. There have been many instances of employees getting fired because the boss didn't like being embarrassed in the blog, even if it is on the employees personal computer in their own time. Courts weigh freedom of speech with the right to protect the company's public image. Companies should add blogging policies to clarify this to employees on hiring and avoid the confusion.

Hate Speech

Hate speech is protected under the first amendment in the U.S. except when hate speech crosses into threats and intimidation, racial slurs, or racial hostility. Hate speech is prohibited in most other countries. Unfortunately the U.S. has become a safe harbor for hate group websites. Civil lawsuits are a powerful remedy that can financially cripple a hate group organization.

Communism and the Internet

Web speech under Communism is difficult to control. Communist China government has 11 agencies overseeing Internet use. They have taken actions to block certain keyword searches and websites, they keep records of users and the web pages they visit. There is video cameras and high tech software in the internet cafés and bars to prevent customers from viewing the 'forbidden' sites. A user must enter an id number in order to use an internet cafe computer. A

blogger is required to sign up under his or her real name, although they can write under a pseudonym. Examples of banned websites are: a pornographic site, a superstitious site, or websites that criticize government or the Communist Party. Dozens of people have been sent to prison for posting or downloading from such sites.

C. E-BANKING

DEFINITION OF E-BANKING

Electronic banking, also known as electronic funds transfer (EFT), is simply the use of electronic means to transfer funds directly from one account to another, rather than by cheque or cash. You can use electronic funds transfer to:

• Have your paycheck deposited directly into your bank or credit union checking account.

• Withdraw money from your checking account from an ATM machine with a personal identification number (PIN), at your convenience, day or night.

• Instruct your bank or credit union to automatically pay certain monthly bills from your account, such as your auto loan or your mortgage payment.

• Have the bank or credit union transfer funds each month from your checking account to your mutual fund account.

• Have your government social security benefits check or your tax refund deposited directly into your checking account.

• Buy groceries, gasoline and other purchases at the point-ofsale, using a check card rather than cash, credit or a personal check.

• Use a smart card with a prepaid amount of money embedded in it for use instead of cash at a pay phone, expressway road toll, or on college campuses at the library's photocopy machine or bookstores.

• Use your computer and personal finance software to coordinate your total personal financial management process, integrating data and activities related to your income, spending, saving, investing, recordkeeping, bill-paying and taxes, along with basic financial analysis and decision making.

VARIOUS FORMS OF E-BANKING:

INTERNET BANKING:

Internet Banking lets you handle many banking transactions via your personal computer. For instance, you may use your computer to view your account balance, request transfers between accounts, and pay bills electronically. Internet banking system and method in which a personal computer is connected by a network service provider directly to a host computer system of a bank such that customer service requests can be processed automatically without need for intervention by customer service representatives. The system is capable of distinguishing between those customer service requests which are capable of automated fulfillment and those requests which require handling by a customer service representative. The system is integrated with the host computer system of the bank so that the remote banking customer can access other automated services of the bank. The method of the invention includes the steps of inputting a customer banking request from among a menu of banking requests at a remote personnel computer; transmitting the banking requests to a host computer over a network; receiving the request at the host computer; identifying the type of customer banking request received; automatic logging of the service request, comparing the received request to a stored table of request types, each of the request types having an attribute to indicate whether the request type is capable of being fulfilled by a customer service representative or by an automated system; and, depending upon the attribute, directing the request either to a queue for handling by a customer service representative or to a queue for processing by an automated system.

AUTOMATED TELLER MACHINES (ATM):

An unattended electronic machine in a public place, connected to a data system and related equipment and activated by a bank customer to obtain cash withdrawals and other banking services. Also called automatic teller machine, cash machine; Also called money machine. An automated teller machine or automatic teller machine (ATM) is an electronic computerized telecommunications device that allows a financial institution's customers to directly use a secure method of communication to access their bank accounts, order or make cash withdrawals (or cash advances using a credit card) and check their account balances without the need for a human bank teller (or cashier in the UK). Many ATMs also allow people to deposit cash or cheques, transfer money between their bank accounts, top up their mobile phones' pre-paid accounts or even buy postage stamps. On most modern ATMs, the customer identifies him or herself by inserting a plastic card with a magnetic stripe or a plastic smartcard with a chip, that contains his or her account number.

The customer then verifies their identity by entering a passcode, often referred to as a PIN (Personal Identification Number) of four or more digits. Upon successful entry of the PIN, the customer may perform a transaction. If the number is entered incorrectly several times in a row (usually three attempts per card insertion), some ATMs will attempt retain the card as a security precaution to prevent an unauthorised user from discovering the PIN by guesswork. Captured cards are often destroyed if the ATM owner is not the card issuing bank, as noncustomer's identities cannot be reliably confirmed. The Indian market today has approximately more than 17,000 ATM's.

TELE BANKING:

Undertaking a host of banking related services including financial transactions from the convenience of customers chosen place anywhere across the GLOBE and any time of date and night has now been made possible by introducing on-line Telebanking services. By dialing the given Telebanking number through a landline or a mobile from anywhere, the customer can access his account and by following the user-friendly menu, entire banking can be done through Interactive Voice Response (IVR) system. With sufficient numbers of hunting lines made available, customer call will hardly fail. The system is bi-lingual and has following facilities offered

- Automatic balance voice out for the default account.
- Balance inquiry and transaction inquiry in all
- Inquiry of all term deposit account
- Statement of account by Fax, e-mail or ordinary mail.
- Cheque book request
- Stop payment which is on-line and instantaneous
- Transfer of funds with CBS which is automatic and instantaneous
- Utility Bill Payments
- Renewal of term deposit which is automatic and instantaneous
- Voice out of last five transactions.

SMART CARD:

A smart card usually contains an embedded 8-bit microprocessor (a kind of computer chip). The microprocessor is under a contact pad on one side of the card. Think of the microprocessor asreplacing the usual magnetic stripe present on a credit card or debit card. The microprocessor on the smart card is there for security. The host computer and card reader actually "talk" to the microprocessor. The microprocessor enforces access to the data on the card. The chips in these cards are capable of many kinds of transactions. For example, a person could make purchases

from their credit account, debit account or from a stored account value that's reload able. The enhanced memory and processing capacity of the smart card is many times that of traditional magnetic-stripe cards and can accommodate several different applications on a single card. It can also hold identification information, which means no more shuffling through cards in the wallet to find the right one -- the Smart Card will be the only one needed. Smart cards can also be used with a smart card reader attachment to a personal computer to authenticate a user. Smart cards are much more popular in Europe than in the U.S. In Europe the health insurance and banking industries use smart cards extensively. Every German citizen has a smart card for health insurance. Even though smart cards have been around in their modern form for at least a decade, they are just starting to take off in the U.S.

DEBIT CARD:

Debit cards are also known as check cards. Debit cards look like credit cards or ATM (automated teller machine) cards, but operate like cash or a personal check. Debit cards are different from credit cards.

While a credit card is a way to "pay later," a debit card is a way to "pay now." When you use a debit card, your money is quickly deducted from your checking or savings account. Debit cards are accepted at many locations, including grocery stores, retail stores, gasoline stations, and restaurants. You can use your card anywhere merchants display your card's brand name or logo. They offer an alternative to carrying a checkbook or cash.

E-CHEQUE:

• An e-Cheque is the electronic version or representation of paper cheque.

• The Information and Legal Framework on the E-Cheque is the same as that of the paper cheques.

• It can now be used in place of paper cheques to do any and all remote transactions.

• An E-cheque work the same way a cheque does, the cheque writer "writes" the e-Cheque using one of many types of electronic devices and "gives" the e-Cheque to the payee electronically. The payee "deposits" the Electronic Cheque receives credit, and the payee's bank "clears" the e-Cheque to the paying bank. The paying bank validates the e-Cheque and then "charges" the check writer's account for the check.

OTHER FORMS OF ELECTRONIC BANKING

• Direct Deposit

• Electronic Bill Payment

• Electronic Check Conversion

• Cash Value Stored, Etc.

BENEFITS/CONCERNS OF E-BANKING BENEFITS OF E-BANKING

For Banks:

Price- In the long run a bank can save on money by not paying for tellers or for managing branches. Plus, it's cheaper to make transactions over the Internet.

Customer Base- The Internet allows banks to reach a whole new market- and a well off one too, because there are no geographic boundaries with the Internet. The Internet also provides a level playing field for small banks who want to add to their customer base.

Efficiency- Banks can become more efficient than they already are by providing Internet access for their customers. The Internet provides the bank with an almost paper less system.

Customer Service and Satisfaction- Banking on the Internet not only allow the customer to have a full range of services available to them but it also allows them some services not offered at any of the branches. The person does not have to go to a branch where that service may or may not be offer. A person can print of information, forms, and applications via the Internet and be able to search for information efficiently instead of waiting in line and asking a teller. With more better and faster options a bank will surly be able to create better customer relations and satisfaction.

Image- A bank seems more state of the art to a customer if they offer Internet access. A person may not want to use Internet banking but having the service available gives a person the feeling that their bank is on the cutting image.

For Customers:

Bill Pay: Bill Pay is a service offered through Internet banking that allows the customer to set up bill payments to just about anyone. Customer can select the person or company whom he wants to make a payment and Bill Pay will withdraw the money from his account and send the payee a paper check or an electronic payment.

Other Important Facilities: E- banking gives customer the control over nearly every aspect of managing his bank accounts. Besides the Customers can, Buy and Sell Securities, Check Stock Market Information, Check Currency Rates, Check Balances, See which checks are cleared,

Transfer Money, View Transaction History and avoid going to an actual bank. The best benefit is that Internet banking is free. At many banks the customer doesn't have to maintain a required minimum balance. The second big benefit is better interest rates for the customer.

CONCERNS WITH E-BANKING

As with any new technology new problems are faced.

Customer support - banks will have to create a whole new customer relations department to help customers. Banks have to make sure that the customers receive assistance quickly if they need help. Any major problems or disastrous can destroy the banks reputation quickly an easily. By showing the customer that the Internet is reliable you are able to get the customer to trust online banking more and more.

Laws - While Internet banking does not have national or state boundaries, the law does. Companies will have to make sure that they have software in place software market, creating a monopoly.

Security: customer always worries about their protection and security or accuracy. There are always question whether or not something took place. Other challenges: lack of knowledge from customers end, sit changes by the banks, etc.

E-BANKING GLOBAL PERSPECTIVE

The advent of Internet has initiated an electronic revolution in the global banking sector. The dynamic and flexible nature of this communication channel as well as its ubiquitous reach has helped in leveraging a variety of banking activities. New banking intermediaries offering entirely new types of banking services have emerged as a result of innovative e-business models. The Internet has emerged as one of the major distribution channels of banking products and services, for the banks in US and in the European countries.

Initially, banks promoted their core capabilities i.e., products, services and advice through Internet. Then, they entered the ecommerce market as providers/distributors of their own products and services. More recently, due to advances in Internet security and the advent of relevant protocols, banks have discovered that they can play their primary role as financial intermediates and facilitators of complete commercial transactions via electronic networks especially through the Internet. Some banks have chosen a route of establishing a direct web presence while others have opted for either being an owner of financial services centric electronic marketplace or being participants of a non-financial services centric electronic marketplace.

The trend towards electronic delivery of banking products and services is occurring partly as a result of consumer demand and partly because of the increasing competitive environment in theglobal banking industry. The Internet has changed the customers' behaviors who are demanding more customized products/services at a lower price. Moreover, new competition from pure online banks has put the profitability of even established brick and mortar banks under pressure. However, very few banks have been successful in developing effective strategies for fully exploiting the opportunities offered by the Internet. For traditional banks to define what niche markets to serve and decide what products/services to offer there is a need for a clear and concise Internet commerce strategy.

Banking transactions had already started taking place through the Internet way back in 1995. The Internet promised an ideal platform for commercial exchange, helping banks to achieve new levels of efficiency in financial transactions by strengthening customer relationship, promoting price discovery and spend aggregation and increasing the reach. Electronic finance offered considerable opportunities for banks to expand their client base and rationalize their business while the customers received value in the form of savings in time and money.

Global E-banking industry is covered by the following four sections:

• **E-banking Scenario**: It discusses the actual state, prospects, and issues related to E-banking in Asia with a focus on India, US and Europe. It also deals with the impact of Ebanking on the banking industry structure.

• **E-banking Strategies**: It reveals the key strategies that banks must implement to derive maximum value through the online channel. It also brings guidance for those banks, which are planning to build online businesses.

• **E-banking Transactions**: It discusses how Internet has radically transformed banking transactions. The section focuses on cross border transactions, B2B transactions, electronic bill payment and presentment and mobile payments. In spite of all the hype, E-banking has been a non-starter in several countries.

• **E-banking Trends:** It discusses the innovation of new technologies in banks.

THE INDIAN EXPERIENCE

India is still in the early stages of E-banking growth and development. Competition and changes in technology and lifestyle in the last five years have changed the face of banking. The changes that have taken place impose on banks tough standards of competition and compliance. The issue

here is – 'Where does India stand in the scheme of E-banking.' E-banking is likely to bring a host of opportunities as well as unprecedented risks to the fundamental nature of banking in India.

The impact of E- Banking in India is not yet apparent. Many global research companies believe that E-banking adoption in India in the near future would be slow compared to other major Asian countries. Indian E-banking is still nascent, although it is fast becoming a strategic necessity for most commercial banks, as competition increases from private banks and non-banking financial institutions.

Despite the global economic challenges facing the IT software and services sector, the outlook for the Indian industry remains optimistic.

The Reserve Bank of India has also set up a "Working Group on E-banking to examine different aspects of E-banking. The group focused on three major areas of E-banking i.e. (1) Technology and Security issues (2) Legal issues and (3) Regulatory and Supervisory issues. RBI has accepted the guidelines of the group and they provide a good insight into the security requirements of E-banking.

The importance of the impact of technology and information security cannot be doubted. Technological developments have been one of the key drivers of the global economy and represent an instrument that if exploited well can boost the efficiency and competitively of the banking sector. However, the rapid growth of the Internet has introduced a completely new level of security related problems. The problem here is that since the Internet is not a regulated technology and it is readily accessible to millions of people, there will always be people who want to use it to make illicit gains. The security issue can be addressed at three levels. The first is the security of customer information as it is sent from the customer's PC to the Web server. The second is the security of the environment in which the Internet banking server and customer information database reside. Third, security measures must be in place to prevent unauthorized users from attempting to long into the online banking section of the website.

From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk.. Regarding the regulatory and supervisory issues, only such banks which are licensed and supervised and have a physical presence in India will be permitted to offer E-banking products to residents of India. With institutions becoming more and more global and complex, the nature of risks in the international financial system has changed.

The Regulators themselves who will now be paying much more attention to the qualitative aspects of risk management have recognized this.

Conclusion

From all of this, we have learnt that information technology has empowered customers and businesses with information needed to make better investment decisions. At the same time, technology is allowing banks to offer new products, operate more efficiently, raise productivity, expand geographically and compete globally. A more efficient, productive banking industry is providing services of greater quality and value.

E-banking has become a necessary survival weapon and is fundamentally changing the banking industry worldwide. Today, the click of the mouse offers customers banking services at a much lower cost and also empowers them with unprecedented freedom in choosing vendors for their financial service needs. No country today has a choice whether to implement E-banking or not given the global and competitive nature of the economy. The invasion of banking by technology has created an information age and commoditization of banking services. Banks have come to realize that survival in the new e-economy depends on delivering some or all of their banking services on the Internet while continuing to support their traditional infrastructure.

The rise of E-banking is redefining business relationships and the most successful banks will be those that can truly strengthen their relationship with their customers.

Without any doubt, the international scope of E-banking provides new growth perspectives and Internet business is a catalyst for new technologies and new business processes. With rapid advances in telecommunication systems and digital technology, Ebanking has become a strategic weapon for banks to remain profitable. It has been transformed beyond what anyone could have foreseen 25 years ago.

Two years ago, E-banking was a strategic advantage, nowadays; it is a business reality, if not a necessity.

UNIT- II

CYBER CRIMES

A. OBSCENITY

Pornography or obscenity is very sensitive issue all over the world yet there is no settled definition of the word under any law. What is nude art or sexually explicit thing for one person may be obscene or porn for another. Hence, it is very difficult to define "What is porn?"

There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect. Classic example is a website,www.incometaxpune.com, prima facie, it looks a website of Income tax department of Pune City, but actually it's a porn site. Though it was blocked many times by law enforcement agencies in India, it is still available with obscene contains.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories (remember "Savitabhabhi"!!!). The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression; it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive".

Section 67 of the Information Technology Act, 2000 penalizes cyber pornography. Other Indian laws that deal with pornography include the **Indecent Representation of Women (Prohibition) Act** and the **Indian Penal Code**.

Section 67 reads as under:-
Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

This section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal.

Explanation
Any material in the context of this section would include video files, audio files, text files, images, animations etc. These may be stored on CDs, websites, computers, cell phones etc.

Lascivious is something that tends to excite lust.
Appeals to, in this context, means "arouses interest".

Prurient interest is characterized by lustful thoughts.
Effect means to produce or cause some change or event.
Tend to deprave and corrupt in the context of this section means "to lead someone to become morally bad".
Persons here refers to natural persons (men, women, children) and not artificial persons (such as companies, societies etc).

To be considered obscene for the purpose of this section, the matter must satisfy at least one of the following conditions:-

- it must tend to excite lust, or
- it must arouse interest in lustful thoughts, or
- it must cause a person to become morally bad.

The above conditions must be satisfied in respect of a person who is the likely target of the material.

Illustration
Sameer launches a website that contains information on sex education. The website is targeted at higher secondary school students. Pooja is one such student who is browsing the said website. Her illiterate young maid servant happens to see some explicit photographs on the website and is filled with lustful thoughts.
This website would not be considered obscene. This is because it is most likely to be seen by educated youngsters who appreciate the knowledge sought to be imparted through the photographs. It is under very rare circumstances that an illiterate person would see these explicit images.

Acts those are punishable in respect of obscenity:-
"**Publishing**" means "to make known to others". It is essential that at least one natural person (man, woman or child) becomes aware or understands the information that is published. Simply putting up a website that is never visited by any person does not amount to publishing.

"**Transmitting**" means to pass along convey or spread. It is not necessary that the "transmitter" actually understands the information being transmitted.

Information **in the electronic form** includes websites, songs on a CD, movies on a DVD, jokes on a cell phone, photo sent as an email attachment etc.

The **punishment** provided under this section is as under:-

- First offence: Simple or rigorous imprisonment up to **3 years** and fine up to **Rs 5 lakh**.

- Subsequent offence: Simple or rigorous imprisonment up to **5 years** and fine up to **Rs 10 lakh**.

Amendments of 2008 introduced new Section on Cyber pornography i.e. **Section 67A**.

The Section makes publishing or transmitting of sexually explicit act or conduct illegal with a punishment of imprisonment upto five years and with fine which may extend to ten lakh rupees for first offence and seven years for subsequent offences.

Hence, the Section makes publishing or transmission of blue films, audio sex clips, pictures, magazines and any other material in the electronic form involving sexually explicit acts illegal.

B. DEFAMATION

INTRODUCTION

Pornography or obscenity is very sensitive issue all over the world yet there is no settled definition of the word under any law. What is nude art or sexually explicit thing for one person may be obscene or porn for another. Hence, it is very difficult to define "What is porn?"

There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect. Classic example is a website,www.incometaxpune.com, prima facie, it looks a website of Income tax department of Pune City, but actually it's a porn site. Though it was blocked many times by law enforcement agencies in India, it is still available with obscene contains.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories (remember "Savitabhabhi"!!!). The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression; it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive".

Section 67 of the Information Technology Act, 2000 penalizes cyber pornography. Other Indian laws that deal with pornography include the **Indecent Representation of Women (Prohibition) Act** and the **Indian Penal Code**.

Section 67 reads as under:-
Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

This section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal.

Explanation: Any material in the context of this section would include video files, audio files, text files, images, animations etc. These may be stored on CDs, websites, computers, cell phones etc.

Lascivious is something that tends to excite lust.
Appeals to, in this context, means "arouses interest".
Prurient interest is characterized by lustful thoughts.
Effect means to produce or cause some change or event.
Tend to deprave and corrupt in the context of this section means "to lead someone to become morally bad".
Persons here refers to natural persons (men, women, children) and not artificial persons (such as companies, societies etc).

To be considered obscene for the purpose of this section, the matter must satisfy at least one of the following conditions:-

- it must tend to excite lust, or
- it must arouse interest in lustful thoughts, or
- it must cause a person to become morally bad.

The above conditions must be satisfied in respect of a person who is the likely target of the material.

Illustration

Sameer launches a website that contains information on sex education. The website is targeted at higher secondary school students. Pooja is one such student who is browsing the said website. Her illiterate young maid servant happens to see some explicit photographs on the website and is filled with lustful thoughts.
This website would not be considered obscene. This is because it is most likely to be seen by educated youngsters who appreciate the knowledge sought to be imparted through the photographs. It is under very rare circumstances that an illiterate person would see these explicit images.

Acts those are punishable in respect of obscenity:-
"**Publishing**" means "to make known to others". It is essential that at least one natural person (man, woman or child) becomes aware or understands the information that is published. Simply putting up a website that is never visited by any person does not amount to publishing.

"**Transmitting**" means to pass along convey or spread. It is not necessary that the "transmitter" actually understands the information being transmitted.

Information **in the electronic form** includes websites, songs on a CD, movies on a DVD, jokes on a cell phone, photo sent as an email attachment etc.

The **punishment** provided under this section is as under:-

•First offence: Simple or rigorous imprisonment up to **3 years** and fine up to **Rs 5 lakh**.

•Subsequent offence: Simple or rigorous imprisonment up to **5 years** and fine up to **Rs 10 lakh**.

Amendments of 2008 introduced new Section on Cyber pornography i.e. **Section 67A**.

The Section makes publishing or transmitting of sexually explicit act or conduct illegal with a punishment of imprisonment upto five years and with fine which may extend to ten lakh rupees for first offence and seven years for subsequent offences.

Hence, the Section makes publishing or transmission of blue films, audio sex clips, pictures, magazines and any other material in the electronic form involving sexually explicit acts illegal.

B. DEFAMATION

Introduction

The law of defamation protects the reputation of individuals and organisations by granting the injured party the right to sue for damages. There is no specific legislation dealing with the issue of defamation on the Internet, but the Defamation Acts cover the field. Each Australian state once took a slightly different legislative approach to defamation. In NSW, the common law applies with significant statutory modifications from the *Defamation Act* 2005 Unless otherwise noted, in this document this is the Act we mean when we use 'Defamation Act'.

There used to be a historical distinction, in the 1974 Act of the same name, between 'libel' and 'slander' (in writing *cf.* verbal) but this no longer exists due to s 7 of the *Defamation Act* 2005.

All Australian states and territories have enacted legislation based on the model uniform defamation legislation, which came into force on 1 January 2006. This legislation aims to retain the existing common law of defamation, except to the extent that it is specifically modified by that legislation.

In general terms the following must be present to establish defamation:

1) a**defamatory statement** (or material) or an **imputation**. Section 8 of the *Defamation Act* 2005 (NSW) requires that imputation is the basis of the cause of action

2) the statement (or material) **identifies** the plaintiff

3) the statement (or material) is **published** to a third person, i.e. at least one person other than the plaintiff. Section 8 requires that the imputation is made by means of its publication.

Defamatory statements or material must be 'published' if there is to be a cause of action.

Once a person views material which has been uploaded, sent or posted on the Internet, that material is regarded as having been published (*Rindos v Hardwick* below).

It is important to note that where a person views the material may determine where publication takes place, which is of significance in determining which court will have jurisdiction. This issue is exemplified in *Dow Jones & Company Inc v Gutnick* [2002]

Courts also consider principals to have published material that has in fact been published by their agent (*Webb v Bloch* (1928) 41 CLR 331). Arnold-Moore in `Legal Pitfalls in Cyberspace: Defamation on computer networks' suggests that this could mean that employers "who are usually the operators of computers…are liable for defamatory statements made by their employees in the course of their employment". However, there is no case law on this matter.

publication is also a recognized form of publication. Taking defamatory material, copying and distributing it may result in a defamation claim against the original writer of the material, as well as the persons who copied and distributed it. If the role of the republisher equates to approval or adoption of the imputation, then it will be considered to be published material (*Hepburn v. TCN Channel 9* [1983] 2 NSWLR 664).

The problem that the Internet creates in this area, is that Internet Service Providers (ISPs) and Internet Content Hosts (ICHs) may be considered publishers or republishers of material carried or hosted by them, even though they may have little if any control over the material that is published.

This means they are potentially liable for defamation anywhere in the world where the material is accessed or republished.

'Mere distributor' and innocent dissemination

The courts distinguish between a publisher and a mere distributor. For example, a newsagent may not be held liable for selling papers that contain defamatory material if they were not aware of what the material contained. The same applies to ISPs, they can avoid liability of it can be proved that they were only a distributor of the material.

See section 8 below for more information, in particular the statutory defence in the *Defamation Act 2005 (NSW)* of 'innocent dissemination'.

Case Study: *Rindos v Hardwick 1994*

Australia's first Internet defamation case was *Rindos v. Hardwick* (Supreme Court of Western Australia, Unreported judgment 940164, 31 March 1994.

It involved a message posted on an international science anthropology bulletin board, in which the defendant made a number of defamatory remarks about the plaintiff in response to a posting which criticized the plaintiff's dismissal by the University of Western Australia. The defamatory remarks included accusing Dr. Rindos of engaging in paedophilia with a young boy, and that he has no academic ability as an anthropologist but rather has advanced his career through the bullying and berating of others.

Ipp J found that material placed on an electronic bulletin board, such as a Usenet group, is indeed 'published' material. (It was the first time in Australia that material placed on the Internet was classified as published material.) His Honor found that posting material on an international bulletin board was sufficient to warrant that it had been published. He noted that:

'These defamatory remarks were published in academic circles throughout the world… the nature of the remarks is such that they are likely to be repeated, and that any rumours of a like kind that had circulated previously were likely to gain strength from their publication *[on the Internet].*'

~~C~~ase study: Dow Jones & Company Inc v Gutnick

On 10 December 2002 the High Court handed down its famous judgement in the case of *Dow Jones & Company Inc v Gutnick* [2002] HCA 56. The appellant, Dow Jones publishes *Wall Street Journal* and *Barrons* magazine and an online news service, *Barrons Online*, the respondent is a prominent Victorian businessman, who while most of his business affairs are conducted in Victoria has overseas interests, including in the Unites States.

On October 28, 2000 Dow Jones had published anarticle 'Unholy Gains' which accused Gutnick of improper business dealings with a convicted tax-evader and money-launderer Nachum Goldberg. The article also appeared on the publisher's website, where it appeared that it had been accessed by numerous Americans and about 300 people in Victoria, as well as 14 people that had purchased the magazine.

Gutnick sued Dow Jones for defamation in the Supreme Court of Victoria, and limited his claim to the loss of reputation he suffered in Victoria.

The principal issue before the Court was whether the defamation action should proceed in Victoria, New York where the article was written or New Jersey where the article was uploaded onto Dow Jones's web servers. While this case is mainly about jurisdiction and the Internet, it is nonetheless relevant to the issue of online defamation.

Gleeson CJ, McHugh, Gummow and Hayne JJ issued a joint judgement in which they held, that the defamation occurred in the place where the damage was suffered, coherent with established legal authority:

> *'It is only when the material is in comprehensible form that the damage to reputation is done… In the case of material on the World Wide Web, it is not available in comprehensible form until downloaded on to the computer of a person who has used a web browser to pull the material from the web server. It is where that person downloads the material that the damage to reputation may be done…that will be the place where the tort of defamation is committed.'*

They also rejected the appellant's claim that if jurisdiction was granted in Victoria then publishers all over the world would potentially be liable to be sued in multiple jurisdictions every time they published something on the Web as being inconsistent with the above principle.

Gaudron J agreed with Gleeson CJ, McHugh, Gummow and Hayne JJ while making further comments about the American 'Single-Publication rule'.

Kirby J while not dissenting adopted a more prudent approach. Noting the global nature of the Internet, he suggested that 'basic *lack of locality suggests the need for a formulation of new legal rules to address the absence of congruence between cyberspace and the boundaries and laws of any given jurisdiction*' (Para 13). Kirby called for both national legislation and the eventual development of an international agreement in the area of Internet defamation.

Callinan J like the others agrees that the defamation case should be heard in Victoria. He notes that 'A *publisher, particularly one carrying on the business of publishing, does not act to put matter on the Internet in order for it to reach a small target. It is its ubiquity, which is one of the main attractions to users…* [Publishers] *are not obliged to publish on the Internet. If the potential reach is uncontrollable then the greater the need to exercise care in publication.'* (atPara 182).

The High Court unanimously dismissed the appeal and Gutnick was now free to sue Dow Jones in Victoria, under Victorian law. He eventually achieved a small settlement ($400k)

Defamatory meaning and imputations:

The courts look at the whole publication when determining whether or not material is defamatory. Thus, the words upon which the plaintiff relies must be looked at in their context.

The material will be defamatory if it exposes someone to hatred, contempt or ridicule. One judge described a defamatory statement as a statement that is "*of a kind likely to lead ordinary decent folk to think less of the person about whom it is made*" (Jordan CJ *Consolidated Trust Co Ltd v Browne* (1948) 49 SR (NSW) 86 at 88). It is not the words that have been used themselves which are said to be defamatory but the meaning that is conveyed by those words. These meanings are known as imputations. To be liable for defamation, the imputations need not be intentional (*John Fairfax & Sons v. Hook* (1983) 47 ALR 477, 481).

The Internet allows users to choose the order in which they view information and so meanings or imputations that were not intended may be drawn by a user. The following are examples:

- words on one website linked to another site; or
- Words on one website linked to images on a different site.

To pursue a claim for defamation, the material must sufficiently identify the plaintiff. A reference to someone as part of a group is sufficient for a claim in defamation provided that the group is a small one. For example, to say that all New South Wales Fraud Squad members are corrupt identifies each of those people whilst to say that all Australians are corrupt does not. A corporation can be defamed by material which harms its trading reputation.

Any person who participates in the publication of defamatory material can be held liable. With publishing on the Internet, the author of the material, the ISP and Internet Content Hosts (ICHs), and any other infrastructure providers may thus be liable. ISP liability arises from the services they provide to customers such as website and newsgroup hosting, and other services where the ISP does not exercise editorial control. If the ISP has the power to remove material (e.g. on newsgroups) or can control how long material is stored, they may be liable if that material is defamatory.

It may not be easy to identify the source of defamatory material published on the Internet. Internet users do not have to register their true identity and it may even be difficult to prove where a person's registered source computer is located. Alternatively, it may be difficult to link that computer with an individual especially where the computer is made available to the general public at, for example, an Internet café. Also some complainants may not be able to recover damages from the author and then will choose to sue the ISP (who generally tend to have more money) in order to recover damages or have the material removed.

ISPs have also been sued when courts have considered them to be publishers (as opposed to mere carriers or distributors) of defamatory material. Whilst there is no clear authority, it would seem that an ISP would be treated as a mere distributor of material unless it can be demonstrated that the ISP knew or ought to have known of the defamatory material which has been uploaded using their service. The defense of innocent dissemination (or innocent publication in NSW) is

available to ISPs who inadvertently distribute defamatory material. This will be covered in more detail in Section 7.

The report *Defamation and the InternetScoping Study No 2* UK Law Reform Commission December 2002 looks at the position of online defamation in the UK as well as making some suggestions for reform. The report revealed that regular practice for ISPs was that once they received notice that a web page contained defamatory material they would remove the entire site as opposed to just the page for fear that the customer would reinstate the page and then the ISP would again be liable. The site would be restored once the customer provided written assurance that they would not repeat the defamatory material. However ISPs complained that they felt uncomfortable in the current climate of legal uncertainty, censoring material which may not be defamatory, and that the process of identifying and removing defamatory material is often time-consuming and costly. Removing material that may turn out not to be defamatory may find the ISP in breach of contract with their customer as well as interfering with the customer's freedom of expression. Suggestions for reform include extending ISP immunity, as has been done in the United States, introducing codes of practice for ISPs to follow and, reforms to s (1) of the *Defamation Act* 1996 (UK).

The Electronic Commerce (EC Directive) Regulations European Union 2002 while not a comprehensive instrument is designed to limit ISP liability on a range of legal issues. The Directive distinguishes between three types of Internet services and affords different liabilities to each:

Mere conduits are in essence the actual telephonic networks. They do not "initiate transmission", "select the receiver" or "modify information". This does not include websites or Usnet as these are stored by the ISP, a further characteristic of mere conduits is that they only store information for as long as it is needed for transmission. Regulation 17 excludes this type of service provider from any liability. This is understandable as mere conduits are simply distributors and do not exercise any editorial control over the material.

- **Caching** refers to the temporary storing of information by ISPs in order to facilitate more efficient operation of the Internet. ISPs are again excluded from any liability; however, if a court orders that defamatory material must be removed the ISP will loose immunity if they fail to do this expeditiously.
- **Hosting** is where an ISP stores information provided by a recipient of the service. This includes those who store web pages and webmail services. Article 19 excludes ISPs from liability provided that, among other things, they have no knowledge of the illegal activity or information, and if the provider gains knowledge of any illegal information or activity they act expeditiously to remove or disable access to the information.

The current position in the US is that "no publisher or user of an interactive computer service shall be treated as the publisher… of any information provided by another information content provider" (s 230(c)(1) *Communications Decency Act* 1996). This means that no ISP is ever liable as a publisher of defamatory material. US courts have also interpreted that a distributor is a type of publisher, extending the protection of s 230(c)(1) to distributors (*Zeran v America Online* 958 F Supp 1124 (ED va, 1997). The First Amendment strongly protects freedom of speech which also restricts the number of defamation claims made in America. Defamations of Stratton Oakmont were published on `Money Talk'. Ain J found Prodigy liable on 2 grounds:

- Prodigy '*exercised sufficient editorial control ... to render it a publisher with the same responsibilities as a newspaper*'(ie not an innocent disseminator like a newsagent). Factors taken into account included: (i) Prodigy's content guidelines; (ii) Prodigy's own use of a screening program for offensive language; (iii) use of Board Leaders; and (iv) technical means to delete after posting. Prodigy also held itself out as a 'family network' that screened content.
- Epstein was Prodigy's agent (ie acting on their behalf and subject to their control), the court found this despite the 'talismanic language' in their agreement that tried to make Epstein not an agent, i.e. the Court looked at the substance of the relationship.

Flaming

Defamation is common in the online world, but is rarely pursued to the stage of litigation. A culture has developed in email discussion lists and chat rooms which accepts that the discussion may be fairly vigorous, frank and even heated. The most common online responses to defamatory material are to ignore it or to return fire. The original defamation is often referred to as 'flaming' and any response might start a 'flame war'. It is rare for these exchanges to end up in the courts.

However, despite the cultural shift towards greater freedom of speech, the traditional law of defamation still applies. The legal resolution will follow the same path as any other defamation action. That is, the three key elements of defamation must be proved (a defamatory imputation must be made, the material must identify the complainant and the material must be published to a third person) and all available defences must be overcome.

While flame wars were rife in the early years of the Internet, now as the Internet has become open to the greater public and has a dominant corporate presence, greater care needs to be taken with what is published online. UK's first e-mail defamation case in July 1997 received extensive media attention. Western Provident Association sued Norwich Union Healthcare for propagating untrue rumours about Western's financial security on its internal e-mail system. The case was settled before reaching court for a substantial £450 000. Lilian Edwards, *Defamation and the Internet: Name Calling in Cyberspace*, 1997

Defenses

A number of defences to defamation exist. These include:

- **absolute privilege**
- **qualified privilege**

Defamation with malice will defeat all defences other than truth of the defamatory material.

Defense of innocent publication

Anyone who posts anything on the Internet effectively publishes that material in every jurisdiction in the world. Unwitting distributors of defamatory material may be absolved from liability through the defense of innocent dissemination. While historically this defense applied to re-distributors such as newsagents and book sellers, it is also a particularly appropriate defense for ISPs.

At common law, the defense of innocent dissemination requires that the defendant:

- Had no actual knowledge of the defamation
- Had no reason to believe the material carried was defamatory
- Was not negligent in that lack of knowledge (*Emmens v. Pottle*(1885) 16 QBD 354, 357, 358).

The*Defamation Act* NSW), provide~~d~~ the defendant make~~s~~ an offer of amends, including an offer to publish a correction and an apology. Where the plaintiff does not accept an offer of amends, the defendant escapes liability if he or she was not the author of the material and can prove 'that the author was not actuated by ill will'.

Reasonableness is a relevant factor in determining whether an ISP has been negligent in failing, for example, to monitor material posted on its bulletin boards. Given the large volume of material on bulletin boards and the speed with which such material is posted, ISP's may argue it is an unreasonable burden to monitor all such material. The issue of what is reasonable in determining negligence becomes more straightforward once an ISP becomes aware of defamatory material posted on its bulletin boards and fails to remove such material within a reasonable time. Once an ISP becomes aware of defamatory material, it is more likely to be held liable if the ISP fails to remove it.

Case Study: *Thompson v Australian Capital Television Pty Ltd & Ors*

In *Thompson v Australian Capital Television* (1996) 186 CLR 574, Channel 7 re-broadcast a live relay of a program produced by Channel 9. The plaintiff subsequently sued the defendant as a re-publisher of the defamatory material and the High Court had to consider whether the defendant could use the defence of innocent dissemination for this television broadcast. The

defamation the plaintiff suffered occurred when his step-daughter claimed on *The Today Show* that he had committed incest with her since she was seven years old, and that he had fathered the child she had at fourteen. No evidence was ever produced to suggest there was any truth in this statement.

The High Court rejected Channel 7's argument that it was an innocent disseminator of the program, stating:

'It is true that Channel 7 did not participate in the production of the original material constituting the program. But Channel 7 had the ability to control and supervise the material it televised... it by no means follows that Channel 7 was merely a conduit for the program and hence a subordinate disseminator. It was Channel 7's decision that the telecast should be near instantaneous, a decision which was understandable given the [current-affairs] nature and title ['The Today Show'] of the program but which was still its decision.'

The court held that a television station, republishing live by relay an interview originally broadcast on another television station, was liable for defamation. The court reasoned that as the defendant *'had the ability to control and supervise the material'* it had effectively authorized the publication, and must thus be classified as an original publisher of the material. The Court held that the defense of innocent dissemination was only available to a defendant who could prove that they were a 'mere distributor'. Only then could the defendant argue that they were unaware of the defamatory material and not negligent in that lack of knowledge. How is this relevant to ISP liability for material published in the Internet? As a result of *Thompson*, ISPs who wish to rely on the defense of innocent dissemination must first prove that they do not have the ability to control Internet content. In *obiter* Brennan CJ, Dawson and Toomey at 10-11 stated *"there is no reason in principle why a mere distributor of electronic material should not be able to rely upon the defense of innocent dissemination if the circumstances so permit"*(at 589). However they did not expand further on this point and it must be noted that it was made in the context of the controlled medium of television broadcasting as opposed to interactive and comparatively unregulated and uncontrolled media of the Internet (Doran *Flaming Liability* 2000). Currently there is no definitive Australian authority on whether ISPs and ICHs rely on the defense of innocent dissemination and if so to what extent.

Case Study: *Godfrey v Demon Internet Ltd*

Godfrey v Demon Internet Limited [1999] 4 All ER 342 relates to a posting made on the newsgroup 'soc.culture.thai' contained on the Demon website. An unknown US resident posing as Dr. Godfrey posted an offensive message, which Morland J described as *"squalid, obscene and defamatory"*. On January 1997 Godfrey sent a fax to the defendant notifying them of the forged imputation and requesting its removal from the Demon server. The defendant failed to do this and the plaintiff subsequently sued for defamation.

The defense sought to rely on the defense of innocent dissemination (s 1(1) *Defamation Act* 1996 (UK)), however this was rejected and the court held that after the ISP became aware of the defamatory material it could not use the innocent dissemination defense. Morland J drew particular attention to the fact that innocent dissemination does not grant ISPs absolute immunity but rather only protects those who are unaware of the defamatory content they are distributing, and are not negligent in doing so. In the end Demon settled the case agreeing to pay the plaintiff damages and costs of £250,000.

This case appears to require ISPs to assess whether material is defamatory if they receive a complaint, but does not place further obligations on an ISP. Nevertheless, it can be difficult for courts to decide whether material is defamatory, let alone ISPs.

Remedies

The main purpose of a defamation action is to compensate a person for harm to his or her reputation. A defamed person may also seek an injunction to prevent dissemination of defamatory material on the Internet. For example, an injunction granted in one jurisdiction against a person who lives in that jurisdiction effectively operates as an injunction on publication (on the Internet at least) throughout the world. However, recent case law demonstrates the reluctance of Australian courts in practice to issue injunctions that would have the effect of restraining publication on the Internet beyond the court's intended jurisdiction. A public apology or retraction is another remedy that is sometimes sought and granted in defamation actions.

Case Study: *Macquarie Bank Ltd &Anor v Berg*

In *Macquarie Bank Ltd v Berg* [1999] NSWSC 526 the plaintiffs are seeking an interlocutory injunction against the defendant preventing him from publishing defamatory material that appeared in macquarieontrial.com and on other Internet sites. While not the main issue, it should be noted that the defendant was not in NSW. Simpson J commented, *"any order made by this court would be enforceable only if the defendant were voluntarily to return to NSW*" (at para 10). The application for the injunction was refused, Simpson J found that:

> *'An injunction to restrain defamation in NSW is designed to ensure compliance with the laws of NSW… Such an injunction is not designed to superimpose the law of NSW… on every other state, territory and country of the world. Yet that would be the effect of an order restraining publication on the Internet… It may very well be that, according to the law of the Bahamas, Tazhakistan, or Mongolia, the defendant has an unfettered right to publish the material. To make an order interfering with such a right would exceed the proper limits of the use of the injunctive power of this court'* (at para 14)

C. HACKING AND CRACKING

Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Those individuals who engage in computer hacking activities are typically referred to as "hackers."

The majority of hackers possess an advanced understanding of computer technology. The typical computer hacker will possess an expert level in a particular computer program and will have advanced abilities in regards to computer programming.

Unlike the majority of computer crimes which are regarded as clear cut in terms of legality issues, computer hacking is somewhat ambiguous and difficult to define. In all forms, however, computer hacking will involve some degree of infringement on the privacy of others or the damaging of a computer-based property such as web pages, software, or files.

As a result of this loaded definition, the impact of computer hacking will vary from a simple invasive procedure to an illegal extraction of confidential or personal information.

Definitions of Hacking

The New Hacker's Dictionary, a resource used to elucidate upon the art of computer hacking, has defined the practice through an assortment of definitions:

A hacker may be defined as any person who enjoys exploring the intricacies of programmable systems and how to stretch their capabilities. This definition is held in contrast to a generic computer user, who prefers to access a computer's minimal functions;

One who programs or who enjoys programming, as opposed to those individuals who simply theorize about programming;

An individual who possesses exceptional skill regarding computer programming;

A malicious meddler who attempts to discover and subsequently tamper with sensitive information through poking around computer-based technologies. These individuals are commonly referred to as "network hackers" or "password hackers."

Regardless of the definition, there are unwritten rules or principles that a hacker will ultimately live by. The belief that information sharing is a powerful exercise and that is the ethical duty of

hackers to share their expertise through the creation of free software and through facilitating access to information and to computing resources is a fundamental code for which the majority of hackers follow. In addition, computer hacking as a practice revolves around the belief that system-cracking as a hobby or for fun is ethically okay so long as the hacker commits no vandalism, theft, or a breach of confidentiality.

Issues of Computer Hacking

Computer hacking possesses a mixed perception. Due to our reliance on computer technologies and the critical information shared on networks, the art of computer hacking has been skeptically viewed. That being said, there is also a "Robin Hood" mentality attached to the practice, where free programs or facilitated measures have been awarded to the average computer user.

The primary issue attached to computer hacking stems from an individual's ability to access crucial or personal information that is found on a computer network. The ability to retrieve and subsequently tamper with such information will give way to the potential to commit heinous criminal acts.

Ways to Prevent Computer Hacking

Educational institutions must clearly establish use policies and delineate appropriate and inappropriate actions to all individuals who access information via a computer. The use of filters or firewalls may be considered to reduce access to unauthorized software serial numbers and other hacking-related materials.

D. CRIME THROUGH MOBILE PHONES:

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

1. 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.
2. 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, and hackers destroy "Property" in the form of computer files or Records.

- Hackers Injure Other Computer Users by Destroying Information Syste
- 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 not 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-crimesare 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 be 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 thisregard. 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 allay 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

UNIT-III

GENETIC AND MEDICAL TECHNOLOGIES

A. REGULATION OF GENETIC TECHNOLOGY

Just as the twentieth century was a golden age of computing, the twenty-first century is the DNA age. The silicon age brought about dramatic changes in how we as species work, think, ommunicate, and play. The innovations of the computer revolution helped bring about the current genetic revolution, which promises to do for life what computing did for information. We are on the verge of being able to transform, manipulate, and create organisms for any number of productive purposes. From medicine, to agriculture, to construction and even computing, we are within reach of an age when manipulating the genetic codes of various organisms, or engineering entirely new organisms, promises to alter the way we relate to the natural world.

Biotechnology, specifically genetic engineering, is already a beneficial resource, employed in medicine, manufacturing, and agriculture. We have begun reaping the practical rewards of genetic engineering such as new medical therapies and increased crop yields and so far only a few instances of measurable harm have resulted. Genetic engineering has the potential to improve our health and well-being dramatically, revolutionize our manner of living, help us to conserve limited resources, and produce new wealth. Provided that it is appropriately regulated, bearing in mind ethical concerns relating to dignity, harmful consequences, and justice, its potential benefits outweigh its harms. There is certainly no reason to reject it outright as "unnatural." Biotechnology should be understood as an extension of already accepted and well-established techniques, such as directed breeding, combined with sophisticated understanding of evolution and genetic technologies.

As with any revolutionary technology, anxieties, fears, and moral objections to the promise of genetic engineering abound. Some are well-grounded and suggest caution, while others are the product of misinformation, religious prejudice, or hysteria. We should sort out those objections based on sound science and reason from those that are unfounded. Given the relative youth of the technology and the tremendous possibilities it offers for improvement of the human condition, as well as the environment in general, careful consideration of ethical implications now can help inform and ensure the future of the genetics era.

As indicated, some significant moral implications ought to be taken into account as we go forward with genetic engineering. Some of the moral implications that we should consider carefully are discussed below in three clusters: first, general ethical concerns, both religious and secular, about the intrinsic immorality of genetic engineering; second, the potential beneficial and harmful consequences of genetic engineering; and finally, issues of justice, especially fair access to genetic therapies and enhancements. Note that given the scope of this paper there are many other ethical issues that are not addressed, such as the ownership of genetic information.

The Basic Science

Deoxyribonucleic acid (DNA) is a remarkable molecule capable of directing the development and propagation of organisms. The organizational component of every life form on Earth is wrapped up in DNA's double-stranded molecular structure. Each organism carries within its

DNA the instructions for that organism's every ongoing function, folded tightly in the nucleus of most of its cells. The same DNA exists in the organism's "germline" cells, used for reproduction, as in the organism's other cells (referred to as somatic cells); however, germline DNA, as opposed to somatic DNA, is used solely to create new offspring, forming a part of the set of instructions that are combined (in the case of sexual reproduction) with DNA from the other parent.

The DNA molecule consists of four nitrogenous bases, adenine, thymine, guanine and cytosine, on a phosphate-sugar "backbone," twisting in a double helix like a spiral staircase. A subunit of DNA, consisting of a base, a phosphate group, and a sugar, is referred to as a "nucleotide." Each thymine base is joined across the "rung" of the double helix ladder to an adenine base, and each cytosine base is joined with a guanine base.

This structure is both elegant and remarkable. Because of the exclusive bonding of these base pairs, replicating a strand of DNA, and thus the instructions for the organism's development and each of its cells' ongoing metabolism, can be accomplished more or less by simply splitting the DNA strand in two down the rungs of the ladder. Each half, split along the axis of its rungs, provides a template that will recombine with loose nucleotides to form exact copies of the original strand, with the help of special "proofreading" enzymes, and some other mechanisms of cellular reproduction.

The genetic code of organisms such as humans is complex, with nearly three billion base pairs. Those three billion base pairs are arranged in different sequences, yielding approximately 25,000 genes, each of which is responsible for some trait or facet of each of us. When combined with environmental factors, variations in the coding of those genes define our unique identities. Not every trait is cosmetic. While genes convey information about features such as hair and eye color, height, etc., they also convey information about important biological functions. Errors in the sequencing of some genes can produce genetic disorders.

There are more than four thousand known genetic disorders. These conditions and diseases may be chronic or degenerative or even latent and undiscovered for some time, but are ultimately harmful to the organism. In some cases, genetic disorders are the result of errors which creep into germline cells because of environmental factors; some errors creep into the genome as a result of copying errors during replication. In other instances, defective genes may be passed on through generations of parents where the trait has not been fatal. In many cases, genetic diseases remain as dormant, recessive traits waiting to be passed on to offspring of parents who both happen to have the recessive characteristic.
Over time, all of these means of genetic change have resulted in the current form of humans. The process of mutation, responsible for the emergence of genetic diseases, is also the underlying mechanism of evolution. Evolution is the process of genetic change over time, as some of these changes result in a fitter version of the species more apt to survive than others, and these advantageous traits are then passed on to succeeding generations. In some cases, the errors conferred a survival advantage in some environments while subsequently conferring a condition classified as a disease in other environments, as with the hemoglobin-s gene, responsible for the sickle-cell trait, which confers some immunity to malaria but also results in anemia.

Most mistakes in DNA replication result in errors in the production of proteins. Somatic cell DNA is essentially a protein-making code that directs cellular metabolism throughout an organism by controlling the production of essential proteins that direct the ongoing survival and functioning of discrete cells in every organ of the body. Because of tissue differentiation mechanisms, also part of the instruction set of DNA, different types of cells in the body produce different types of proteins. Certain genes in those organs are "turned on" and others are "turned off," directing the tissues of those organs to perform their own unique functions. Genetic diseases typically involve mistakes in an organism's DNA sequence that results in disruption in the normal production of a certain protein.

While the actual mechanisms of genetic diseases are complex, scientists are learning more about their causes and how to detect them. Some of the relevant DNA changes occur in the gene causing the disease; other changes, while not present in the directly relevant gene, alter the functioning of that gene; a third type of change, while not causing a particular disease, indicates that the individual with that particular sequence is more susceptible to developing the disease. Many of these changes can now be detected and scientists continue to discover correlations between specific DNA sequences and genetic diseases. By understanding these correlations, scientists could test for the presence of a particular disease, or the susceptibility to that disease, and perhaps devise cures based upon our knowledge of these relationships.
Besides the promise of treating or curing genetic diseases, manipulating DNA can enable scientists to develop new strains of organisms, including mice that serve as models of human diseases useful for pharmaceutical testing, or sheep that secrete medicines in their milk. New strains of agricultural crops have been engineered, by inserting genes from animals or other plants, making them resistant to cold, disease, or pesticides . In sum, as we learn about the specific functioning of genes in various species, we are able to develop new, useful life forms; manufacture new medicines; and improve human life, health and the environment.

But these medicines, therapies, and other products of genetic engineering present ethical challenges. For purposes of understanding these challenges, it is useful to distinguish different categories of genetic intervention. They are:

- Somatic gene therapy, which aims at the treatment or prevention of disease without affecting future generations, and is the least morally objectionable; somatic genetic enhancement, which aims to improve the functioning of the individual;
- germline gene therapy, which aims at preventing disease, but involves heritable genes; and germline genetic enhancement, which aims to improve the functioning of future generations.

Ethical Concerns

1. Objections to Genetic Engineering as Inherently Wrong
Some people object to any tinkering with the genetic codes of humans, or even of any life form. Some religious critics perceive genetic engineering as "playing God" and object to it on the grounds that life is sacred and ought not to be altered by human intention. Other objectors argue from secular principles, such as the outspoken and ardent Jeremy Rifkin, who claims that it

violates the inherent "dignity" of humans and other life-forms to alter their DNA under any circumstances.

a) Religious objections to genetic engineering

Arguments based upon life's sacredness suggest that altering life forms violates the will of a creator (Ramsey 1966, p.168), but they fail for want of internal theoretical consistency or because they rest on question-begging assumptions. If a creator does exist, most philosophers and theologians agree that either the creator's will is expressed in every facet of its creation, or that consistent with the creator's will mankind has free will, which includes the ability to create technologies (for a contrary view, see Prather 1988, pp.138–42). Thus, either genetic engineering can be seen as an expression of the creator's will—since it forms part of creation—or it is the result of our having been imbued with free will.

Clothing, agriculture, and weaponry have existed since before the dawn of civilizations,and each alters our relationship with nature. These technologies express a rejection of the"natural" order of things, and result from human consciousness and intentionality. Infact, embracing these technologies has altered human evolution, enabling us to ventureoutside of the savannah, and live in a variety of climates, defending ourselves frominclement environments and dangerous predators. Without these technologies, it is likelythat humans would look very different, with different strengths and weaknesses fromthose we see now, and would have remained in relatively restricted environments insteadof populating six out of the seven continents (and the seventh to a limited extent). Assuch, the history of our tinkering with the natural is long, and its results generally laudedby religious and secular alike.

Technologies such as antibiotics and contraceptives have interfered with thenatural order of evolution, preventing the conception of millions of human beings, andenabling the survival of others who might have died through exposure to diseases. Thesetechnologies have affected not only human populations, but also numerous species wherehumans have interfered through medicines, contraception, and selective breeding. Thosewho oppose the alteration of genomes of humans and other species based upon somenotion of the inviolability of natural processes must provide an ethical justification of theuse of medicines, contraception, and selective breeding which somehow sets them apartfrom conscious, more targeted alterations at the genetic level. The technical differencebetween genetic engineering and these other mechanisms of altering the natural evolutionof various species is the difference between a blunderbuss and a rifle. The blunderbussapproach we have historically taken, by the use of contraception, antibiotics, andselective breeding, results in unanticipated consequences: medical and social problemsmay result from selecting for certain traits by breeding, or by ensuring the survival ofpotentially unfit members of the species through the use of medicines, or even bypreventing generations of potentially fit members of a species being born. Moreover,these techniques are not always reliable in achieving their desired results. By contrast,genetic engineering is a rifle that can be accurately focused on a desired target.Admittedly, genetic engineering may have undesired side effects as well, but, asindicated, this does not distinguish this technique from currently accepted methods.

b) Secular objections to genetic engineering

Secular objectors to genetic engineering must defend the claim that the dignity of an individual member of a species, or of the species itself, is tied to its unhampered-with evolution to its present state. This claim seems difficult to defend in light of the great infirmities—arguably indignities—that occur because of evolution, which is utterly indifferent to the suffering that results from many genetic disorders. Wholly innocent creatures lead lives of illness or degradation, or die prematurely because of genetic diseases. Nature itself is indifferent to our dignity, and so altering nature cannot violate our dignity. In fact, it dignifies us to use the talents we have to alter our environment and our biology to improve our lives and those of the disabled. Technology in any form is an outgrowth of our intellectual abilities: at its best, it allows us to overcome natural shortcomings. Home heating and air conditioning violate the natural order, yet allow us to thrive in climates we otherwise could not survive. Few would argue that overcoming that natural disadvantage violates our inherent dignity.

Those who argue for drawing a line at altering the genome of humans or other organisms must give reasons both for regarding DNA as somehow special and apart from the rest of the natural world *and* for arguing that conscious manipulation of DNA is morally impermissible. There are some reasons to support "genetic exceptionalism," the point of view that DNA is unique, but those arguments do not necessarily imply: a) that because of this uniqueness there are absolute bars to altering it; or b) that if it is acceptable to alter the DNA of non-humans, it is nonetheless unacceptable to alter that of humans. Uniqueness does not itself imply any moral duty. In fact, every human being is "unique" by virtue of DNA, environment, and upbringing, but our moral duties toward each do not depend upon that uniqueness. Neither of the assumptions above can be sustained by logic or empirical evidence, and, as indicated previously, we have beentinkering with genes in plants, animals, and even human beings, through selective breeding for millennia.

2. Benefits and Drawbacks of Genetic Engineering

a) Benefits

Genetic engineering has already supplied us with products that alleviate illness,clean up the environment, and increase crop yields, among other practical benefits tohumanity and the ecosystem. For example, the first genetically engineered life form to begranted patent protection was developed byAnandaChakrabarty, who geneticallyengineered a common bacterium into Burkholderiacepacia, a variant that digestspetroleum products. He obtained a patent for his new life form, and helped establish theSupreme Court precedent that, to this day, enables inventors to patent geneticallyengineered life forms (Diamond v. Chakrabarty 1980). The bacterium cleans up oil spillsand has proven to be both safe and useful. Since this precedent, tens of thousands ofpatents have issued for genetically engineered life forms.

Genetic engineering has also helped create thousands of organisms and processesuseful in medicine, research, and manufacturing. Genetically engineered bacteria churnout insulin for treating human diabetes, production of which would be substantially #75797027) was the first genetically engineered

mouse to be patented for use as a modelfor cancer research. Numerous other "knock-out" mice have followed, each missingcertain critical genes, or expressing certain genetic diseases, so that medical researcherscan test drugs and other treatments for human genetic maladies without risking the livesof human subjects, and reducing the numbers of experimental animals sacrificed forscience in the process. Gene therapy, in which manufactured viruses can deliver repairsto somatic cells with genetic defects, is making strides to correct genetic diseases ordefects in fully grown humans.

Genetically engineered foods produce pest-resistant and drought-resistant crops,reducing the need for pesticides and fertilizers, and increasing yields in a world with anever-growing need for food. Much of the so-called "green revolution" of the past fewdecades has been fueled by standard chemical technologies. New pesticides and remotesensing have enabled reductions in the amount of hazardous chemicals entering theecosystem, and allowed farmers faced with an ever-expanding human population to meetthe food needs of a planet. Nonetheless, insects and fungi, through evolutionarydynamics, develop resistance to pesticides. Moreover, even the best modern pesticidesenter the food chain and the ecosystem, harming generations of humans and animalsalike. Even in European countries like The Netherlands, farmers have recently had toswitch from soil-growing plants to hydroponics due to the accumulation of toxic saltsfrom fertilizers and pesticides (Levine and Suzuki 1993, p.176). The promise of newgenetic engineering technologies includes the development of pest-resistant strains ofcrops that would require little-to-no pesticides, or robust drought-resistant plants that cangrow in harsh environments without irrigation (Levine and Suzuki 1993, pp.185–86).

Genetic engineering also holds the promise of creating new, more productivestrains of farm animals for meat and milk production. These new strains may be moreresistant to infections, reducing the need for large, unhealthy doses of antibiotics(McCreath 2000, pp.1068–69). They may also be engineered to produce more meat, sowe need not slaughter as many animals, or they may produce milk or other products withvital nutrients otherwise not found in those products, ensuring a healthier source of suchnutrients. Eventually, as envisioned in Margaret Atwood's Oryx and Crake (2003),animal variants used as food sources might even be engineered without anything more expensive without the use of genetic engineering. The OncoMouse (U.S. Patentthan an autonomous nervous system, arguably eradicating many of the ethical concernsinvolved with the wholesale slaughter of large mammals for food.

b) Drawbacks

Of course, we need to assess our actions in light of both short and long-termconsequences to the biosphere. Although the scientific consensus is that geneticengineering poses few, if any, short-term threats to the environment, long-term threats,known and unknown, must be considered as we move forward with research and genetictechnologies.

As mentioned in the brief introduction to the science underlying geneticengineering, somatic-cell and germline genetic engineering differ in important ways.Somatic cell therapy seeks to repair damage to cells that are not gametes. A creature witha genetic disease could theoretically be cured by somatic-cell

therapy, and some advanceshave recently been made. One of the principal disadvantages of this process is itscomplexity. Repairing a fully grown organism means altering the genetic makeup ofliving cells.

Genetic engineering has made the most progress in germline alterations where thegametes of the organisms contain the altered DNA, and thus the organism's offspringcarry the altered traits. This is the sort of engineering which has resulted in nearly everymajor scientific breakthrough and technological offshoot of genetic engineering. Altered bacteria, knock-out and other experimental animal models, andcommercially available crops are among those that have resulted from germline geneticengineering.

Altering germ cells is a process that requires caution. Fertile organisms withaltered germ cells may propagate beyond our control. This has happened with somegenetically altered crops which have, in some instances, cross-fertilized non-engineeredcrops and spread their altered genes. This happened with Monsanto's "Terminator" corn,which renders its offspring infertile: farmers who chose not to use Monsanto's seedsnevertheless suffered the effects of infertile crops and could not use a portion of theircrops to reseed because they had interbred with "Terminator" corn. Seeds of neighboring non-genetically modifiedcrops were "terminated" by cross-pollination, although the effects seem to have beenlimited to the first generation (Ruiz-Marerro 2002).

Moreover, because of the complexity of most genomes, all the consequences of aparticular gene's alteration often cannot be predicted. In particular, how a geneticallymodified plant or animal might interact with other living things cannot be known forcertain until it is placed in the wild, and, at that point, effective control over theseinteractions may not be possible. The controversy surrounding Bt-corn illustrates some ofthe possible dangers from genetically modified organisms. Bt-corn has genes from thebacterium Bacillus thuringiensis (Bt) spliced into it. The alteration is effective against theEuropean corn borer, thus eliminating the need for excessive use of pesticides. The cornwas shown to be safe for human consumption, but had an unanticipated and unintendedconsequence. In 1999, a Cornell study showed that the corn produced a toxin fatal to thelarvae of monarch butterflies and this toxin could be found in the corn's pollen. Furthermore, as is often the case with plants in the wild, pollen from Btcornspread to surrounding plants, including milkweed, which is a source of nutrition forthe butterfly larvae. Fortunately, subsequent studies have shown that the toxin is notsufficiently concentrated in field conditions to pose any significant harm to monarchbutterfly populations (Sears et al. 2001). Nonetheless, no one had anticipated thisproblem, which illustrates how difficult it is to rein in the spread of pollen and thereby, insome cases, the spread of altered genes.

This dramatic incident underscores the potential for significant harm to theenvironment from genetic engineering, especially in this nascent phase where we areoften unable to predict the consequences of germline genetic enchancement. Germlinealterations, as opposed to somatic alteration, affect the gametes and thus propagatealterations, in unpredictable ways, to future generations of the altered species. Once agermline alteration is introduced into a species, evolution takes over for successivegenerations. Evolution, as we know, is unpredictable. The complexity of calculatingpotential successive generations exceeds our present knowledge about genes and theirinteractions not only

epigenetically, with the environment, but also generationally, withother members of the species with which the progeny may interbreed. It requires thatscientists and commercial producers of genetically altered life forms take particular careto explore all the possible effects of their products, not just on humans, but upon thebiosphere as whole. Currently, we have only educated guesses and interpolation frompast examples of genetically altered species, but over time, as computing technologyimproves, those guesses will be refined. In the meantime, germline alterations should becarefully introduced in isolated communities so that generational effects can be evaluatedfor the dangers of a release of altered organisms in the wild.

Another dramatic example of specific harm from genetic engineering is the caseof Jesse Gelsinger, who died shortly after an experimental gene therapy treatment for agenetic liver disease (Corzin and Kaiser 2005, p.1028). Although that case involved aresearch trial of an experimental protocol, it is conceivable that future gene therapiesmight introduce harmful effects into the gene pool, not necessarily resulting in death, butaffecting future generations. The important lesson learned from this and other actual

harms caused by experimental and even commercial genetic engineering is that therelationships between genes and phenotypes are far more complex than we currentlyunderstand. It behooves us to do adequate research and risk calculus for germlinealterations that may affect all successive generations of a species.

New bioinformatics and modeling technologies should enable greater caution.Laboratory testing as well as field experience should be employed to forestall furtherharm to the biosphere. Assessing the actual risks of genetic technologies is fastbecoming a major concern for scientists working in this area:

The basic features of general risk assessment of GMOs [geneticallymodified organisms] are understandably different from those associatedwith chemicals. Genetically modified organisms are living organisms andtherefore, unlike chemicals that may become diluted, GMOs have thepotential to disperse to new habitats, colonize those sites, and multiply.

Their novel activities, including the production of metabolic products,enzymes and toxins will occur as long as the GMOs remain metabolicallyactive. Once established, living organisms cannot be recalled. One voluntary organization currently compiling and disseminating data for use inrisk assessment is the International Centre for Genetic Engineering and Biotechnology(ICGEB) (www.icgeb.org). The organization has 55 member countries, not including theUnited States, who jointly fund research centers in India, South Africa and Italy, withheadquarters in Trieste. The organization maintains databases of genetically modifiedproducts in use, adverse field reports, and relevant statistics, as well as biosafety trainingand risk assessment tools for scientists engaging in genetic engineering research andapplications.

As the tools for data gathering and modeling for genes, organisms andpopulations improve, so too should the practical use of risk assessment. Appropriate riskassessment will help minimize adverse consequences.

3. Justice and Equity

Ethical principles and concerns about justice should act as a check ontechnological advancement. As distinct from science, which ought to be free toinvestigate any area of nature without restriction, technology brings scientificadvancements that impact both humanity and the planetary environment for good or forill. Apart from direct benefits or harms that may result from genetic engineering, whichwe have already considered, there is also the problem of how genetic engineering mayaffect the distribution of social goods as well as political rights. Such issues are oftenreferred to as problems of distributive justice. This paper cannot take on the task ofdefining and defending a comprehensive theory of justice; however, we will take as agiven that great disparities of wealth and power are not, all other things being equal,desirable. They are especially undesirable if they result in great disparities of politicalpower.

With the onset of genetic engineering, there is a concern that geneticinterventions, especially genetic enhancements —or the reverse, deliberate geneticdisabling—may exacerbate already existing inequities as well as creating new ones. Inevaluating these concerns, we need to bear in mind that genetic engineering is still young.Some of the possibilities discussed, such as creating new species of superhumans orsubhumans, seem highly unlikely, at least for the foreseeable future. We are a long wayfrom developing H.G. Wells-style Morlocks to serve as our slaves. Nonetheless, although mad-scientist examples seem extreme, they are used by those whoargue against the morality of using genetic engineering, and because many of theseexamples are within the range of technical possibility, they serve as useful illustrationsfor the underlying principles.

Beyond science-fiction examples, immediate issues involving access and socialstratification impact on current notions of justice and should be worked out in public debate, perhaps legislation. As with any new and expensive medicaltechnology, non-socialized medical regimes in which genetic interventions becomeavailable will likely result in stratification of services and beneficiaries. There will bethe class of those who can afford access to new technologies, and those who cannot. Thiswill not be a unique situation, for already a number of elective and even necessarymedical procedures are unavailable to the segment of the population that cannot affordthem, or has inadequate or no health insurance. Inequality of access raises obvious socialjustice concerns where treatments or services are medically necessary which might not beavailable to everyone because of cost.

As with cosmetic enhancements presently available, genetic enhancementsthreaten to create a class division between the “haves” and “have-nots.” Even now,cosmetic surgery confers some tangible economic and social benefits on those who canafford it. While a genetic underclass of slaves seems far-fetched, consider, for instance,parents who decide they want their child to be a NBA (National Basketball Association)player, so they select for traits conferring height, stamina and intense athleticism. Such agenetically enhanced individual will enjoy benefits that no amount of training couldprovide for the most motivated, unenhanced person. In such a possible future, one of themeans by which poor yet motivated people now move from an underclass position to oneof economic security may well

disappear, given unfair competition from players whoseparents could afford genetic enhancement. Similar scenarios can be envisioned for arange of abilities, including intelligence, musical ability, physical attractiveness, etc.Although possession of these traits now confers some social and economicadvantage, it is now the result of chance and evolution (which is largely unpredictable).

In a world where genetic enhancement is available but not readily affordable, only therich will be able to stack the deck in favor of their children.Of course we face similar social-ethical issues with other technologies, but in therealm of genetic modification, decisions are more complex. Cosmetic enhancements arenot hereditable, but the possibility of a new genetic aristocracy is both technicallyfeasible and troubling. However, we must also recognize that it will be difficult tocoordinate and establish rational oversight and regulation of germline modifications inhumans while respecting both autonomy and the need to guard against social injustice.

There is a presumption that self-improvement is permissible, if not laudable, even when itprovides someone with a competitive advantage for herself and her offspring. We wouldregard as unacceptable legislation prohibiting someone from going to law school ormedical school merely because she comes from a wealthy family and can easily affordthe tuition. If use of one's money for a superior education is permissible, can weconfidently say that use of one's money to alter one's genes to obtain a higher IQ foroneself and one's offspring is impermissible? For now, the technology is nowhere nearmarketable, so we have time for a clearheaded dialogue about the social justice issuesassociated with genetic modification by choice.

CONCLUSION:

Bioengineering has the potential to transform our lives in many positive ways.Rejection of this new technology on the ground that it is unnatural or inherently immoralis unwarranted and seems to be based on little more than an instinctive adverse reaction.Biotechnology is an extension of already accepted and well-established techniques, suchas directed breeding, but with the distinct advantage of producing more predictable andmore rapid results. There are risks involved with this new technology, but provided that itis appropriately regulated, its potential benefits outweigh its harms.

Legislators and other responsible decision-makers should not implementregulations that unduly restrict implementation of genetic engineering. In particular,existing mechanisms that ensure the safety of testing protocols should be sufficient forsomatic genetic therapies for humans. With respect to germline enhancements for plantsand animals, we recommend a better coordinated effort among relevant regulatoryagencies, such as the Food and Drug Administration and the Department of Agriculture,to ensure there are no gaps in the regulatory framework. Enhanced organisms should berigorously evaluated and tested in isolated conditions prior to their release in the wild.

Germline alterations for humans should not be prohibited outright, certainly not inadvance of their availability. However, given the special risks posed by human germlinealterations, each proposed

alteration needs to be carefully evaluated, not just with respectto immediate benefits and harms, but also with respect to the effects that the proposedalteration may have on our social structure and the distribution of social goods.

Some have compared genetic engineering to a Pandora's box. If mythologicalanalogies are appropriate, the Center for Inquiry believes a better one would be acomparison to the gift of fire from Prometheus: genetic engineering can provide immensebenefits provided it is used prudently and carefully regulated and controlled.

B. LAWS ON MEDICAL TECHNOLOGY

Communication is a basic link in the patient doctor relationship. Successful communication of information improves the patients under-standing of the diagnosis and increases adherence to therapeutic recommendations and interventions. The ways and means of communication of information have changed with time. From the traditional face to face talk we have now advanced to computer aided communication via Internet, the "Information Highway"(IH).

Networking of four computers by the Advanced Research Projects Agency of the United States Department of Defense created the first Internet in the year 1969. In October 1990, a young scientist Tim Berner-Lee working on the European Particle Physics Laboratory in the Swiss Alps produced the internet's first browser called World Wide Web (WWW). During the last 10 years it has grown into an extensive network of computers spanning the entire globe. Initially, the facility was available to few due to the high cost of the hardware and software, but now it has broken all barriers and is available to millions of people all around the world. The internet has now reached a stage where practically every aspect of human life including health, law, entertainment, communication, commerce, science, etc., is represented in some form or other. The current Internet users worldwide are around 140 million and in our country the number estimated is about 15 million. These figures are changing rapidly due to tremendous popularity currently being enjoyed by this technology. It is estimated that the number of net user worldwide will grow to 350 million by the year 2003. Gross estimates also indicate that a quarter of the data on the Internet is health related and about one third of surfers are searching for this information. A large percentage of such users are medical professionals, who utilize internet not only for quick access of medical information, but also to communicate and advise their patients, sitting in their home/clinic/chamber at click of mouse. The proliferation of electronic data within the modern health information infrastructure pre-sents significant benefits to health care providers and patients, including enhanced patient autonomy, improved clinical treatment based on advances in health research, public health surveillance and modem security techniques. However, there are some reservations about this technology, such as: (a) quality of information; (b) limited availability in local languages; (c) emergence of new syndromes; (d) self-medication hazards; (e) increased consumerism; and (f) increased litigations. In this context, one issue is that of medical confidentiality, which has posed a threat to the basic ethics of the doctor-patient relationship. Presently, world-wide a dozen of countries have cyber laws including India where The Information Technology Act, 2000 was notified on October 17, 2000. But unfortunately, these also do not address the issue of medical confidentiality specifically, although they have provisions related to breach of confidentiality and privacy. To overcome this lacuna, the US Congress has even proposed enactment of comprehensive medical legislation. The initial draft of the said legislation was recently made available for public comment.

Medical Confidentiality

Medical confidentiality is believed to be one of the basic ethics for a physician since ancient time. It was perhaps Hippocrate who first described medical confidentiality as, "whatever, in connection with my professional practice, or not in connection with it, I may see or hear in the lives of men which ought not to be spoken abroad, I will not divulge as reckoning that all should be kept secret". Presently, in the era of high tech information technology this environment of confidentiality is fast changing. The situation of one doctor, one patient and one medical file belongs to the past. Patients records have become computer based, linked to clinical decisions making systems and are accessible to subsequent health care providers irrespective of time and place. Health data about individuals are among the most sensitive types of personal information. Computerized data bases of personally identifiable information may be accessed, changed, viewed, copied, used, disclosed or deleted more easily by more people (both authorized and unauthorized) than paper based records(6). As the access to patient record is not limited to those involved in the health care delivery and patient management, they can be retrieved and used secondarily for different purposes like: (a) education (classroom teaching and conferences); (b) regulation (limitation, post marketing surveillance and accreditation); (c) commercial enterprises (development of biotechnology and marketing strategies); (d) social services and child protection (medical records of spouse or child abuse); and (e) public health services (reports on disease mortality and morbidity, partner notification and surveil-lance. Since each of the researchers has different aim of search on the vast amount of health and personal information available on the information highway, there is every likelihood of breach in privacy. For example, millions of patients records are scrutinized each year by pharmaceutical benefit management (PBM) companies that have overt financial interest in manipulating prescribing practices. Patients are usually not told that these entities have access to their records. A recent survey suggests that they would object, if this was brought to their knowledge.

Electronic mail (e-mail) is gaining popularity in our country also though in recent years it has increased dramatically in the western and developed world. E-mail can be an effective communication tool with the advantage that it: (a) circulates information efficiently; (b) enables thoughtful exchanges of medical information; (c) allows authorized receivers to save messages electronically or in paper form; and (d) can be linked to other educational websites. However, e-mail in the medical context not only generates liability concerns but also raises serious questions about privacy, confidentiality, and authenticity of authorship and patient consent.. E-mail poses threat to confidentiality as others can interrupt unsecured e-mail en route. Anyone having access to a doctor's e-mail account can access, alter and even respond to an e-mail with the illusion of authority.

Another area of concern apart from electronic patient files and e-mail is tele-medicine. Telemedicine uses communication technologies to deliver health care information and services between medical care providers and patients separated by geographical boundary. Telemedicine improves clinical care standard to underserved population, broadens access to speciality care and advanced technology, and facilitates clinical encounters and educational activities between physicians and patient. Yet, it is also not free from the risk of invasion of privacy of the patient, e.g., the patient identifiable information can be sent in telemedicine through interceptable tele-communication having risks of breaching patient-physician confidentiality.

Additionally, some physicians have established web site for the purpose of paid diagnosis. Even though some of these sites invite transmission of specific, identifiable patient data, only a few doctors operated sites are protected by secure servers or encryption technology (the software that scrambles the message in transit and requires an authentication code for both transmission and reception and hence the data/message can be sent/retrieved only by the authorized persons and

not by anybody else. Thus, there are fair chances of breach in confidentiality even in the web communication. Even though, technological safeguards in electronic communication like encryption software can render electronic messages relatively secure, technology alone cannot ensure its legal and ethical use in medical practice. Thus, a physician should adhere to the legal and ethical standards while communicating electronically. The American Medical Association (AMA) has suggested guidelines for its members for AMA web sites.

Physician's Role in Medical Confidentiality

The sensitive nature of the medical information makes it more deserving for special protection. The duty to preserve confidentiality resides with the holder of the record which may not be limited to a single primary care physician alone. Medical files are never free from undue access. The risk is more pertinent with electronic patient file. This risk has potentials to disrupt the fiduciary relationship between the patient and doctor, rather than supporting it(21). Thus, the physician who uses electronic files and e-mail must ensure reasonable precautions to avoid exposing patient's data specially related to identity to unauthorized entities. Moreover, physicians should caution patients against using e-mail for those matters that patients themselves would not wish to be available to payers, employers and other.

The patient should be made aware of the potential risk and benefits of using electronic communication methods. Further, the patients should be informed about the potential ramification of e-mail use, storage and retention, prior to agreeing or declining. It is always advisable to have an informed consent from the patient prior to communication via electronic means. Different countries have enacted laws to maintain the communication privacy such as Electronic Communications Privacy Act of USA, which also includes electronic communications. The consent form should have all the necessary details of the methodology and pros and cons of the technology. While sending a consulting e-mail to a colleague, physicians should refrain from mentioning several cases in one message and may submit unrelated personal messages under separate cover. All patients related e-mail messages should be notified confidential. Physicians who are not prepared to respond to e-mail regularly may decide not to offer this facility to their patients. Privacy has been found only where the sender and recipient have exclusive access to their messages with no risk whatsoever that anyone else could retrieve the information. The Internet whose gateways are numerous and often unpredictable prior to transmitting a message and the providers of on line services may have access to the messages of their subscribers without specific warning. Yet, there is strong social expectation of confidentiality in electronic communication, which could ultimately be legally enforced. So, the physicians should raise their voice individually as well as collectively (through professional associations/societies) to keep this issue of medical confidentiality in the cyber laws of their country. India is among a dozen countries of world and second in whole of Asia to have Information Technology (IT) Act (cyber related law). The act was passed by Parliament on May 17, 2000, and got the President's approval on June 9, 2000. The act came in force on October 17, 2000 when Government issued notification to this giving legal sanctity to e-documents. Section 72 of the act that deals with breach of confidentiality and privacy states "Save as otherwise provided in this act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made thereunder, has secured

access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. But, this act is also silent on the special nature of medical confidentiality. Thus till the time it is incorporated in the act, physicians should adhere to the basic principles of medical confidentiality strictly in order to avoid ethical as well as legal repercussions.

Concluding Comments

Information highway has created a new social relationship between the patient and physicians. The traditional human contact to develop trust and render medical diagnosis might be replaced by electronic and impersonal means. Communication via electronic means may be legal, efficient and even cost effective but is bound to reshape the way medical care is delivered. Physicians and patients alike will resist and perhaps alter their expectations of face to face or voice to voice medicine(18). At present there are fair chances of breach in the patient's confidentiality while interacting through Internet, e-mail and web though it can be minimized, by using more vigil while communicating electronically. Adequate legal protection of personally identifiable health data is necessary to facilitate the transmission of electronic data through e-mail, telemedicine and other routes. Existing legal safeguards are however inadequate and fragmented with major gaps in coverage. Thus, while communicating electronically, it is pertinent for a doctor to adhere to the ethical principles pertaining to patient-physician relationship. Further, enact-ment of comprehensive and uniform cyber law related to the following should be considered to safeguard the patients right to privacy: (a) the unique status of identifiable health information; (b) providing privacy safeguards based on fair information practices (c) empowering patients with information and rights of consent; (d) limiting the disclosure of health related data; and (e) incorporating industry wide security protections(5)

UNIT- IV

BROADCASTING

A. REGULATION AND CONTROL OF BROADCASTING

Main regulatory issues

The main considerations are:

- **Authorisation.** Does the provider need any licences, or to notify or get permission from any regulatory authorities?
- **Content.** Are there any rules governing the content of the service?

- **Competition.** Do any competition rules apply?

Authorisation

Broadcasting Act licence

A television or radio broadcast provider needs a license from Ofcom, the communications regulator, under the *Broadcasting Act 1990* or *1996*. The main licensable services are:

- Television broadcasting services as defined in *section 362* of the Communications Act 2003 (for example, those provided by the ITV companies, Channel 4 and Five).
- Television licensable content services (TLCS) as defined in *section 232* of the Communications Act, which include services broadcast by satellite or distributed over an electronic communications network (ECN) (such as cable or the internet), and which consist of television programmes or electronic programme guides (EPGs).
- Digital television programme services, which are similar to TLCSs but are provided with a view to being broadcast in digital form from a multiplex (a block of transmission capacity).

Licences are also required for other related services such as, for example, local television services and teletext services. There is also a range of radio licences, for digital radio, community radio and radio restricted services.

The detailed distinctions between the different types of broadcast licensable services are beyond the scope of this note, and anyone applying for a license should consult the relevant legislation and the licensing section of Ofcom's website. The distinctions are important, as the license conditions differ for the different types of services. Some services will need more than one Broadcasting Act license to cover their various activities.

"Fit and proper person"

Section 3(3) of both the 1990 and the 1996 Broadcasting Acts requires that licensees are "fit and proper persons". Ofcom sought to explain how it understands this test in the context of considering whether BSkyB remained a fit and proper person to hold a broadcasting licence in the wake of alleged phone hacking by News Corporation newspapers in the summer of 2011. Ofcom published frequently asked questions (see *Legal update, Ofcom publishes "fit and proper person" FAQs*) and a decision on BSkyB (see *Legal update, Ofcom decides Sky is fit and proper broadcast licensee*).

ATVOD notification

Video-on-demand providers have to notify the Authority for Video on Demand (ATVOD) if their service is an "on-demand programme service" (ODPS) under *section 368A(1)* of the Communications Act as amended by the *Audiovisual Media Service Regulations 2009* (*SI 2009/2979*), that is, it provides public "television-like" programmes on-demand under editorial control. ODPS providers must notify ATVOD before beginning to provide ODPS and before ceasing to provide them (*section 368BA, Communications Act*), and pay a fee. For more details, see *Practice note, Video-on-demand*.

Premium-rate services

Broadcasters and other media content providers who use premium-rate services (PRS) within programmes, for example, for voting or competition entry, must register with PhonepayPlus, the premium-rate phone regulator, as they are "level 2" providers under the PhonepayPlus Code of Practice. For more information, see *Practice note, Premium-rate phone services*.

BBC

The BBC operates under Royal Charter, which sets out the public purposes of the BBC, guarantees its independence, and outlines the duties of the Trust and the Executive Board. The current Charter runs until 31 December 2016.

An Agreement with the Secretary of State sits alongside the Charter. It provides detail on many of the topics outlined in the Charter and also covers the BBC's funding and its regulatory duties. The Agreement together with the Charter, establishes the BBC's independence from the government.

Content regulation

The applicable content regulation varies depending on the type of content service being broadcast. The rules are also different depending on the method of transmission, for example, whether the content is part of a scheduled television programme, or available "on demand" over the internet. There are rules for programmes and rules for commercial references (advertisements) within programmes. The source for many of the rules for audiovisual media (scheduled television or on-demand) in the UK is the *Audiovisual Media Services Directive 2007 (2010/13/EU (codified)*) (AVMS Directive).

Programmes

A number of statutory rules and codes apply to programmes. In addition, programmes must comply with the laws on copyright and defamation. Television and online audiovisual programmes are protected by copyright as films under the *Copyright, Designs and Patents Act 1988*, and there is copyright in a broadcast signal to protect the broadcast itself. For more information, see *Practice note, Overview of Copyright*. For information on defamation,

see *Practice note, Overview of defamation*. Call-TV quiz shows must comply with the *Gambling Act 2005* (see *Practice note, Overview of broadcast content regulation: Gambling*).

Broadcasting Act licensees

The following codes apply:

- **Broadcasting Code.** The Broadcasting Code, which is drawn up by Ofcom under *section 319* of the Communications Act, includes standards for television and radio programmes with regard to under-18s, harm and offence, crime, religion, impartiality, accuracy, fairness and privacy, and so on. Ofcom considers allegations of breach of the code and can impose statutory sanctions, including requiring a broadcaster to broadcast a correction or statement of Ofcom's findings, or pay a fine, or have a broadcastinglicense shortened or revoked.

- **Code on Sports and other Listed and Designated Events**. This code ensures that certain free-to-air broadcasters are guaranteed rights to live coverage of key sporting events and other events of national interest.

- **Cross-promotion Code.** This code, which is incorporated into the Broadcasting Code, requires that cross-promotions on television are kept distinct from advertising, and that promotions on television outside programmes must not prejudice fair and effective competition. For more information, see *Practice note, Overview of broadcast content regulation: Ofcom Broadcasting Code*.

- **Code on Electronic Programme Guides**. This code gives guidance on the practices EPG providers should follow, such as giving prominence for public service channels.

- **Code on Television Access Services**. This code sets out requirements on subtitling, sign language and audio description.

BBC

The BBC is subject to some but not all of the requirements of the Broadcasting Code. For example, it is not subject to the rules on impartiality and accuracy, which are covered by the BBC's own *Editorial Guidelines*, and complaints about the BBC's standards compliance are dealt with by the BBC's Editorial Complaints Unit. The House of Lords has noted that the procedure for complaining about BBC content is complex and has suggested that it should be reformed (see *Legal update, House of Lords report on governance and regulation of BBC*).

<u>Public service broadcasters</u>

ITV1, Channel 4, Five and S4C1 are required to provide public service broadcasting as set out in *section 264(4)* of the Communications Act, that is:

- Programmes that deal with a wide range of subjects.

- Television services likely to meet the needs and satisfy the interests of as many different audiences as practicable.

- Television services that meet the needs and interests of the available audiences.

- Maintain high standards with respect to the contents of programmes, the quality of programme making and the skill and editorial integrity applied in making programmes

On-demand services and other internet regulation

- **Programme standards**. On-demand programme services must comply with standards set out in *section 368E* of the Communications Act as amended by the 2009 Regulations. In particular, they must not contain material likely to incite hatred based on race, sex, religion or nationality. If an ODPS contains material which might seriously impair the physical, mental or moral development of persons under the age of 18, the material must be made available in a manner which secures that such persons will not normally see or hear it. On 1 December 2014, new sub-sections 368E(2)-(7) came into force to add detail on what is restricted by section 368E and explicitly prohibiting on-demand programmes services (ODPS) from showing material that the British Board of Film Classification (BBFC) has refused to classify, and restricting ODPS from showing material with an R18 classification certificate unless the material is made available in a way that secures that under 18s will not normally see or hear it. For more information, see *Legal update, Government tightens rules on adult material on VOD*.

- **Internet copyright**. Sections 3 to 16 of the *Digital Economy Act 2010* impose obligations on ISPs aimed at reducing online infringement of copyright by introducing new sections 124A to 124M in the *Communications Act*. ISPs must:

  - Notify their subscribers if their internet protocol (IP) addresses are reported (in a copyright infringement report (CIR) in a prescribed form) by copyright owners as being used to infringe copyright.

  - Provide, on an anonymous basis, copyright infringement lists to copyright owners in relation to subscribers about whom the number of CIRs has exceeded a threshold.

  These obligations are to be subject to and underpinned by an "initial obligations" code of practice, although the first subscriber notifications are unlikely to be sent out before late 2015 (see *Legal update, First copyright infringement notification period under Digital Economy Act 2010 to be delayed until late 2015*).

- **Press regulation**. In September 2014, the Independent Press Standards Organization (IPSO) commenced a voluntary scheme of regulation of most of the national and regional press, replacing the functions of the Press Complaints Commission (PCC). IPSO is likely to regulate audiovisual online material in the same way as the PCC, although it hasn't published anything specific on this. For more information, see *Practice note, Video-on-demand: Press regulation*.

Commercial references

Broadcasting Act licensees

- **Broadcasting Code: sections 9 and 10.** Sections 9 and 10 contain the rules for commercial references in television and radio programming respectively.
  In the case of television, the rules are intended to ensure editorial independence; maintain a distinction between editorial and advertising content; protect audiences from surreptitious advertising; protect consumers; and prevent unsuitable sponsorship. In particular, section 9 deals with:

  - **Product placement.** Product placement is allowed in films, series made for television, sports programmes, light entertainment programmes and programmes acquired from abroad, except that it is prohibited entirely from news programmes and children's programmes. For more on product placement, see *Practice note, Product placement*.

  - **Sponsorship.** Sponsorship must be clearly separated from advertising, and sponsorship credits must not contain advertising messages or encourage the purchase or rental of goods or services. News and current affairs programmes must not be sponsored. For more on sponsorship, see *Practice note, Overview of broadcast content regulation: Advertising and sponsorship*.

  - **Premium-rate services.** For broadcasters using PRS for audience voting and competition entry, section 9.26 requires that where a broadcaster invites viewers to take part in or otherwise interact with its programmes, it may only charge for such participation or interaction by means of PRS or other telephony services based on similar revenue-sharing arrangements. Rule 9.28 says that any promotion of a PRS must be subsidiary to the primary editorial purpose of the programme. Rule 9.29 (and rule 10.9 for radio) requires broadcasters using PRS numbers to comply with the PhonepayPlus Code of Practice (for more information, see *Practice note, Premium-rate phone services*).
    For radio, section 10 ensures the transparency of commercial communications to secure consumer protection.

- **BCAP Code.** The Broadcast Committee of Advertising Practice regulates the content of all television advertisements broadcast by channels and stations licensed by Ofcom, as well as advertisements on interactive television services, television shopping channels and televisual text services, through its code. The code is based on the principles of consumer protection and social responsibility. Compliance with the code is policed by the Advertising Standards Authority. For more on this, see *Practice note, Overview of broadcast content regulation: BCAP Code*. Most broadcasters submit adverts to Clearcast to check compliance with the BCAP Code.

- **Quantity and distribution of advertising.** Ofcom regulates the distribution of advertising breaks through the Code on the Scheduling of Television Advertising (COSTA). The rules on the frequency with which a programme can be interrupted by an advertising break depends on the category of programme, and the requirement not to not to jeopardize the programmer’s integrity, to take account of natural breaks and not to prejudice the rights of the rights-holder. There are

stricter limits on interrupting films made for television, cinematographic works, children's programmes and news programmes. For more on this, see *Practice note, Overview of broadcast content regulation: Code on the Scheduling of Television Advertising*.

- **Teleshopping.** Teleshopping (or "home shopping") is subject to most of the same rules that apply to television advertising. The rules on scheduling teleshopping are contained in COSTA. For more information, see *Practice note, Overview of broadcast content regulation: Teleshopping*.

On-demand services and other internet regulation

ODPS have to comply with rules for advertising, sponsorship and product placement in sections *section 368F*, *368G* and*368H* of the Communications Act respectively, which are enforced by the ASA (for more information on these rules.

Some video-on-demand programming will also be subject to the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (CAP Code), although the Code expressly does not cover website content including editorial content or news unless it otherwise falls under areas to which the Code does expressly apply. Clearcast also checks VOD advertising for compliance with the CAP Code.

Jurisdiction

Under the *AVMS Directive*, audiovisual media services transmitted by a media-service provider under the jurisdiction of a particular EU member state have to comply only with the laws applicable to audiovisual media services in that member state (*Article 2(1), AVMS Directive*). The AVMS Directive provides mechanisms aimed at preventing service providers establishing themselves in a member state where the regulatory regime is more relaxed than the regime in the country in which they wish to broadcast. A member state who considers that a broadcaster under the jurisdiction of another member state provides a television broadcast which is wholly or mostly directed towards its territory can take action to seek to get the broadcaster to comply with the stricter rules (*Article 4, AVMS Directive*).

An audiovisual programme made outside the EU after 19 December 2009 will still have to comply with the basic UK standards in order to be broadcast in the UK. A programme made for reception outside the EU does not have to comply with the AVMS Directive (*Article 2(6), AVMS Directive*) or UK legislation, but may be subject to non-EU regulatory regimes.

Keeping copies

Broadcasting Act licenses contain conditions requiring broadcasters to keep copies of programmes for 90 days in the case of television programmes and 42 days in the case of radio programmes (*section 334, Communications Act*).

ODPS providers must keep copies of all programmes for at least 42 days after the day on which the programme ceases to be available for viewing (*section 368D(3)(zb), Communications Act*).

Competition

The following are a few specific points about competition in the broadcasting sector. Competition law in general is beyond the scope of this note.

Ofcom's principal duties include a duty to further the interests of consumers in relevant markets, where appropriate by promoting competition (*section 3(1)(b), Communications Act*).

Ofcom can impose conditions on a Broadcasting Act license-holder to ensure fair and effective competition between services (*section 316, Communications Act*).

Responsibility for competition matters in the communications sector is shared between Ofcom and the Competition Markets Authority (CMA). Ofcom has concurrent powers with the CMA to exercise Competition Act powers (*section 371, Communications Act*) and can apply and enforce Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU).

Ofcom also has concurrent powers with the CMA in relation to market investigations and super-complaints under the *Enterprise*, insofar as they relate to communications matters (*section 370, Communications Act*). Ofcom can refer completed or anticipated mergers to the Competition Markets Authority to consider whether a merger may be expected to result in a substantial lessening of competition within the appropriate market (*sections 22 and 33, Enterprise Act*). .

Media public-interest consideration

The Secretary of State can intervene in a merger if they think that there is a relevant public-interest consideration (*section 42, Enterprise Act*). Where this is a media public-interest consideration, the Secretary of State can ask Ofcom to report on the consideration (*section 44A, Enterprise Act*). The media public-interest considerations are:

- The need, in relation to every different audience in the UK or in a particular area or locality of the UK, for there to be a sufficient plurality of persons with control of the media enterprises serving that audience.
- The need for the availability throughout the UK of a wide range of broadcasting which (taken as a whole) is both of high quality and calculated to appeal to a wide variety of tastes and interests.

- The need for persons carrying on media enterprises, and for those with control of such enterprises, to have a genuine commitment to the attainment in relation to broadcasting of the standards objectives set out in *section 319* of the Communications Act 2003.

B. LAW RELATING TO CABLE TELEVISION NETWORKING

INTRODUCTION

Cable Television is the talk of the day. In each and every corner of the country people talk about it. Urbanites have the privilege to enjoy the cable television has spread its wings with the results that there has been a haphazard mushrooming of cable television networks all over the country due to availability of signals of foreign television networks via satellites. The programmes which are being projected on the satellite channels are predominantly western and are alien to our culture and way of life. On these cable television networks lot of undesirable programmes and advertisements are also being screened without any fear of being checked. To check this tendency it has been considered necessary to regulate the operation of cable television networks in the country so as to bring about uniformity in theiroperation.
On 29th September, 1994 an Ordinance titled the Cable Television Networks (Regulation) Ordinance, 1994 was promulgated by the President to provide for the regulation of the operation of cable television networks in the country.

The Ordinance was re-promulgated by the President on 17th January, 1995.

To replace the said Ordinance a Bill was introduced in the Parliament which was passed by both of the houses.

STATEMENT OF OBJECTS AND REASONS

1. There has been haphazard mushrooming of cable television networks all over the country during the last few years as a result of the availability of signals of foreign television networks via satellites. This has been perceived as a "cultural invasion" in many quarters since the programmes available on these satellite channels are predominantly western and totally alien to our culture and way of life. Since there is no regulation of these cable television networks, lot of undesirable programmes and advertisements are becoming available to the viewers without any kind if censorship.

2. It is also felt that the subscribers of these cable television networks, the programmers and the cable operators themselves are not aware of their rights, responsibilities and obligations in respect of the quality of service, technical as well as content-wise, use of material protected by copyright, exhibition of uncertified films, protection of subscribers from anti-national broadcasts from sources inimical to our national interest, responsiveness to the genuine grievances of the subscribers and perceived willingness to operate within the broad framework of the laws of the

land.e.g. The Cinematograph Act, 1952, the Copyright Act, 1957, Indecent Representation of Women (Prohibition)Act, 1986.

3. It is, therefore, considered necessary to regulate the operation of cable television networks in the entire country so as to bring about uniformity in their operation. It will, thus, enable the optimal exploitation of this technology which has the potential of making available to the subscribers a vast pool of information and entertainment.

4. The Bill seeks to achieve the above objects.

-

CHAPTER 1

PRELIMINARY

1. Short title, extent and commencement.- (1) This Act may be called the Cable Television Networks (Regulation)Act, 1995.
(2)It extends to the whole of India.
(3)It shall be deemed to have come into force on the 29th days of September, 1994.

2.Definitions. In this Act, unless the context otherwise requires,-

(a) "cable operator" means any person who provides cable service through a cable television network or otherwise controls or is responsible for the management and operation of a cable television network;

(b) "cable service" means the transmission by cables of programmes including retransmission by cables of any broadcast television signals ;

(c) "cable television network" means any system consisting of a set of closed transmission paths and associated signal generation, control and distribution equipment, designed to provide cable service for reception by multiple subscribers ;

(d) "company" means a company as defined in section 3 of the Companies Act, 1956 (1 of 1956);

(e)"person" means- an individual who is a citizen of India ;
(ii) an association of individuals or body of individuals, whether incorporated or not, whose members are citizens of India ;
(iii)a company in which not less than fifty-one per cent. of the paid-up share capital is held by the
citizens of India ;

(f) " prescribed" means prescribed by rules made under this Act ;

(g)"programme" means any television broadcast and includes-
(1) exhibition of films, features, dramas, advertisements and serials through video cassette recorders or videocassetteplayers ;
(ii) any audio or visual or audio-visual live performance or presentation, and the expression " programming service" shall be construed accordingly;

(h) "registering authority" means such authority as the Central Government may, by notification in the Official Gazette, specify to perform the functions of the registering authority under this Act ;

(i)"subscriber" means a person who receives the signals of cable television network at a place indicated by him to the cable operator, without further transmitting it to any other person.

CHAPTER II

REGULATION OF CABLE TELEVISION NETWORK

3. Cable television network not to be operated except after registration.- No person shall operate a cable television network unless he is registered as a cable operator under this Act : Provided that a person operating a cable television network, immediately before the commencement of his Act, may continue to do so for a period of ninety days from such commencement ; and if he has made an application for registration as a cable operator under section 4 within the said period, till he is registered under that section or the registering authority refuses to grant registration to him under that section.

4. REGISTRATION AS CABLE OPERATOR.-(1) Any person who is operating or is desirous of operating a cable television network may apply for registration as a cable operator to the registering authority.

(2) An application under sub-section (1) shall be made in such form and be accompanied by such fee as may be prescribed.

(3) On receipt of the application, the registering authority shall satisfy itself that the applicant has furnished all the required information and on being so satisfied, register the applicant as a cable operator and grant to him a certificate of such registration. Provided that the registering authority may, for reasons to be recorded in writing and communicated to the applicant, refuse to grant registration to him if it is satisfied that he does not fulfill the conditions specified in clause (e)of section 2.

Programme Code. -No person shall transmit or re-transmit through a cable service any programme unless such programme is in conformity with the prescribed programme code:

Provided that nothing in this section shall apply to the programmes of foreign satellite channels which can be received without the use of any specialised gadgets or decoder.

6. Advertisement Code.- No person shall transmit or re-transmit through a cable service any advertisement unless such advertisement is in conformity with the prescribed advertisement code:
Provided that nothing in this section shall apply to the programmes of foreign satellite channels which can be received without the use of any specialised gadgets or decoder.

Maintenance of register.- Every cable operator shall maintain a register in the prescribed from indicating therein in brief the programmes transmitted or re-transmitted through the cable service during a month and such register shall be maintained by the cable operator for a period of one year after the actual transmission or re-transmission of the said programmes.

Compulsory transmission of two Doordarshan channels.- (1) Every cable operator using a dish antenna or Television Receiver only shall, from the commencement of this Act, re-transmit at least two Doordarshan channels of his choice through the cable service. (2) The Doordarshan channels referred to in sub-section (1) shall be re-transmitted without any deletion or alteration of any programme transmitted on such channels.

Use of standard equipment in cable television network -No cable operator shall, on and from the date of the expiry of a period of three years from the date of the establishment and publication of the Indian Standard by the Bureau of Indian Standards in accordance with the provisions of the Bureau of Indian Standards Act, 1986 (63 of 1986), use any equipment in his cable television network unless such equipment conforms to the said Indian Standard.

Cable television network not to interfere with any telecommunication system. - Every cable operator shall ensure that the cable television network being operated by him does not interfere, in any way, with the functioning of the authorized telecommunication systems.

CHAPTER III

SEIZURE AND CONFISCATION OF CERTAIN EQUIPMENT

Power to seize equipment used for operating the cable television network.- (1) If any officer, not below the rank of a Group 'A' officer of the Central Government authorized in this behalf by the Government (hereinafter referred to as the authorized officer), has reason to believe that the provisions of section 3 have been or are being contravened by any cable operator, he may seize the equipment being used by such cable operator for operating the cable television network.

(2) No such equipment shall be retained by the authorized officer for a period exceeding ten days from the date of its seizure unless the approval of the District Judge, within the local limits of whose jurisdiction such seizure has been made, has been made, has been obtained for such retention.

Confiscation-The equipment seized under sub-section (1) of section 11 shall be liable to confiscation unless the cable operator under section 4 within a period of thirty days from the date of seizure of the said equipment.

Seizure or confiscation of equipment not to interfere with other punishment.-No seizure or confiscation of equipment referred to in section 11 or section 12 shall prevent the infliction of any punishment to which the person affected thereby is liable under the provisions of this Act.

Giving of opportunity to the cable operator of seized equipment.- (1) No order adjudicating confiscation of the equipment referred to in section 12 shall be made unless the cable operator has been given notice in writing informing him of the grounds on which it is proposed to confiscate such equipment and giving him a reasonable opportunity of making a representation in writing, within such reasonable time as may be specified in the notice against the confiscation and if he so desires of being heard in the matter :

Provided that where no such notice is given within a period of ten days from the date of the seizure of the equipment, such equipment shall be returned after the expiry of that period to the cable operator from whose possession it was seized.

(2) Save as otherwise provided in sub-section (1), the provisions of the Code of Civil Procedure, 1908 (5 of 1908) shall, so far as may be, apply to every proceeding referred to in sub-section (1)

Appeal.- (1) Any person aggrieved by any decision of the court adjudicating a confiscation of the equipment may prefer an appeal to the court to which an appeal lies from the decision of such court.
(2) The appellate court may, after giving the appellant an opportunity of being heard, pass such order as it thinks fit confirming, modifying or revising the decision appealed against or may send back the case with such directions as it may think fit for a fresh decision or adjudication, as the case may be, after taking additional evidence if necessary.
(3) No further appeal shall lie against the order of the court made under sub-section (2).

CHAPTER IV

OFFENCES AND PENALTIES

Punishment for contravention of provisions of this Act. - Whoever contravenes any of the provisions of this Act shall be punishable,-

(a) for the first offence, with imprisonment for a term which may extend to two years or with fine which may extend to one thousand rupees or with both :

(b) for every subsequent offence, with imprisonment for a term which may extend to five years and with fine which may extend to five thousand rupees.

An offence punishable under clause (a) is non-cognizable and bailable where an offence punishable under clause (b) is cognizable and non-bailable.

(2) Notwithstanding anything contained in sub-section (1), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any negligence on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

CHAPTER V

MISCELLANEOUS

Power to prohibit transmission of certain programmes in public interest.- where an officer, not below the rank of a Group 'A' officer of the Central Government authorized by the State Government in this behalf, thinks it necessary or expedient so to do in the public interest, he may, by order, prohibit any cable operator from transmitting or retransmitting or retransmitting any particular programme if it is likely to promote, on grounds of religion, race, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill-will between different religious, racial, linguistic or regional groups or castes or communities or which is likely to disturb the public tranquility.

Text books:

1. Relevant Legislations and Conventions
2. Information Technology Act - Prof. S.R.Bhansali
3. Cyber Law (Text and Cases), Gerald R. Ferrera, WEST THOMSON LEARNING
4. Cyber Crime - Vakul Sharma