1) INTRODUCTION AND HISTORY OF CYBER LAW

Introduction to Cyber Law

Cyber law is a term that encapsulates the legal issues related to use of communicative transactional, and distributive aspects of networked information devices and technologies.

It is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several sections of the IPC vide the IT Act, 2000, several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC.

Cyber law encompasses laws relating to:

- Cyber Crimes
- Intellectual Property
- Data Protection and Privacy
- Electronic and Digital Signatures

Need for Cyber Law

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.

Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.

Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

Cyberspace is absolutely open to participation by all. A ten-year-old in Bhutan can have a live chat session with an eight-year-old in Bali without any regard for the distance or the anonymity between them.

Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

Cyberspace offers never-seen-before economic efficiency. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

Electronic information has become the main object of cyber crime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds .

A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.

History of Cyber Law in India

- The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce on International Trade Law.
- The Department of Electronics (DoE) in July 1998 drafted the bill.
- However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed.
- It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations.
- The Ministry of Law and Company Affairs then vetted this joint draft.
- After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members.
- The Standing Committee made several suggestions to be incorporated into the bill.
- Suggestions approve by the Ministry of IT were incorporated.
- Cyber café debate. Suggestion dropped in final draft.

---

7) COMPUTER CRIMES

Cyber Crimes Actually Means: It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site. Cyber crimes are not limited to outsiders except in case of viruses and with respect to security related cyber crimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cyber crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

- **Classifications Of Cyber Crimes:** Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cyber crime and what is the conventional crime so to come out of this confusion, cyber crimes can be classified under different categories which are as follows:

1. Cyber Crimes against Persons:

There are certain offences which affects the personality of individuals can be defined as:

- Harassment via E-Mails: It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.
- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- **Cracking:** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.
- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. Crimes Against Persons Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right

of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.

- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.
- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorised person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

3. Cybercrimes Against Government:

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen

as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

4. Cybercrimes Against Society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- **Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

Affects To Whom: Cyber Crimes always affects the companies of any size because almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security risks. In the modern cyber world cyber crimes is the major issue which is affecting individual as well as society at large too.

Need of Cyber Law: information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online interaction expands,

there is expansion in the cyber crimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime. In the modern cyber technology world it is very much necessary to regulate cyber crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

Penalty For Damage To Computer System: According to the Section: 43 of 'Information Technology Act, 2000' whoever does any act of destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine upto 1crore to the person so affected by way of remedy. According to the Section:43A which is inserted by 'Information Technology(Amendment) Act, 2008' where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. And Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Case Study-Attacks on Cyberspace:

- **Worm Attack:** The Robert Tappan Morris well Known as First Hacker, Son of former National Security Agency Scientist Robert Morris, was the first person to be prosecuted under the 'Computer and Fraud Act, 1986'. He has created worm while at Cornell as student claiming that he intended to use the worm to check how large the internet was that time. The worm was uncontrollable due to which around 6000 computer machines were destroyed and many computers were shut down until they had completely malfunctioned. He was ultimately sentenced to three years probation, 400 hours of community service and assessed a fine of $10500. So there must be strict laws to punish the criminals who are involved in cyber crime activities.
- **Hacker Attack:** Fred Cohen, a Ph.D. student at the University of Southern California wrote a short program in the year 1983, as an experiment, that could "infect" computers, make copies of itself, and spread from one machine to another. It was beginning & it was hidden inside a larger, legitimate program, which was loaded into a computer on a floppy disk and many computers were sold which can be accommodate at present too. Other computer scientists had warned that computer viruses were possible, but

Cohen's was the first to be documented. A professor of his suggested the name "virus". Cohen now runs a computer security firm.

- **Internet Hacker:** Wang Qun, who was known by the nickname of "playgirl", was arrested by chinese police in the Hubei province first ever arrest of an internet hacker in China. He was a 19 year old computing student, arrested in connection with the alleged posting of pornographic material on the homepages of several government-run web sites. Wang had openly boasted in internet chat rooms that he had also hacked over 30 other web sites too.

Preventive Measures For Cyber Crimes:

Prevention is always better than cure. A netizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes which can be defined as:

- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programmes by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

Computer Crime Law - US

- Communications Assistance for Law Enforcement Act (CALEA)

  In response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance, Congress enacted CALEA on October 25, 1994. CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities.

- Computer Software Privacy and Control Act

  To prevent deceptive software transmission practices in order to safeguard computer privacy, maintain computer control, and protect Internet commerce.

- Department of Justice - Computer Crime and Intellectual Property Section

  The Computer Crime and Intellectual Property Section (CCIPS) is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. The Computer Crime Initiative is a comprehensive program designed to combat electronic penetrations, data thefts, and cyberattacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.

- Digital Millennium Copyright Act

  The Digital Millennium Copyright Act (DMCA) was enacted in 1998. The basic purpose of the DMCA is to amend Title 17 of the United States Code and to implement the World Intellectual Property Organization (WIPO)

Copyright Treaty and Performances and Phonograms Treaty, which were designed to update world copyright laws to deal with the new technology.

- Economic Espionage Act (EEA)

  In addition to laws specifically tailored to deal with computer crimes, traditional laws can also be used to prosecute crimes involving computers. For example the Economic Espionage Act (EEA) was passed in 1996 and was created in order to put a stop to trade secret misappropriation.

- Electronic Communications Privacy Act

  Passed in 1986, Electronic Communications Privacy Act (ECPA) was an amendment to the federal wiretap law, the Act made it illegal to intercept stored or transmitted electronic communication without authorization.

- FBI - Cyber Crime Division

  The FBI's cyber mission is four-fold: first and foremost, to stop those behind the most serious computer intrusions and the spread of malicious code; second, to identify and thwart online sexual predators who use the Internet to meet and exploit children and to produce, possess, or share child pornography; third, to counteract operations that target U.S. intellectual property, endangering our national security and competitiveness; and fourth, to dismantle national and transnational organized criminal enterprises engaging in Internet fraud. Pursuant to the National Strategy to Secure Cyberspace signed by the President, the Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime.

- Fraud and Related Activity in Connection with Computers

  Section 1030(a)(1) makes it illegal to access a computer without authorization or in excess of one's authorization and obtain information about national defense, foreign relations, or restricted data as defined in the Atomic Energy Act of 19549, which covers all data concerning design, manufacture or utilization of atomic weapons and production of nuclear material. It is worth noting that section 1030(a)(1) requires proof that the individual knowingly accessed the computer without authority or in excess of authorization for the purpose of obtaining classified or protected information. Section 1030(a)(1) criminalizes the use of a computer to gain access to the information, not the unauthorized possession of it or its transmission.

- Fraudulent Online Identity Sanctions Act

  FOISA attempts to tackle the problem of criminals registering online domains under false identification, it includes a provision that would increase jail times for people who provide false contact information to a domain name registrar and then use that domain to commit copyright and trademark infringement crimes.

- Internet Freedom Preservation Act of 2008

  To establish broadband policy and direct the Federal Communications Commission to conduct a proceeding and public broadband summits to assess competition, consumer protection, and consumer choice issues relating to broadband Internet access services, and for other purposes.

- National Information Infrastructure Protection Act of 1996

  The National Information Infrastructure Act (NIIA) was passed in 1996 to expand the CFAA to encompass unauthorized access to a protected computer in excess of the parties' authorization.

- The Computer Fraud and Abuse Act

  The Computer Fraud and Abuse Act, first enacted in 1984 and revised in 1994, makes it certain activities designed to access a "federal interest computer" illegal. These activities may range from knowingly accessing a computer without authorization or exceeding authorized access to the transmission of a harmful component of a program, information, code, or command. A federal interest computer includes a computer used by a financial institution, used by the United States Government, or one of two or more computers used in committing the offense, not all of which are located in the same State. The Legal Institute provides Title 18 of the U.S. Code, which encompasses the Computer Fraud and Abuse Act.

Computer Related Crimes Law

- CAN-SPAM Act

  Despite its name, the CAN-SPAM Act doesn't apply just to bulk email. It covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," including email that promotes content on commercial websites. The law makes no exception for

business-to-business email. That means all email – for example, a message to former customers announcing a new product line – must comply with the law.

- Computer Crime Research Center - Computer Piracy

  Computer piracy is reproduction, distribution and use of software without permission of the owner of copyright. Kinds of illegal software use that can be qualified as copyright violation: - selling of computer facilities with illegally installed software; - replication and distribution of software copies on information carriers without permission of the copyright owner; - illegal distribution of software through communication networks (Internet, e-mail, etc.); - illegal use of software by the user.

- Computer Hacking Laws

  The news said that another person had their identity stolen. It happened again. You might even know of someone that had it happen to them. We often hear of percentages - and they are surprisingly high. Enforcement is taking place, but we have to wonder if computer hacking laws are really having any effect against cyber hacking. This article will show what is being done against cyber crime.

- CyberStalking and CyberHarassment Laws

  States have enacted "cyberstalking" or "cyberharassment" laws or have laws that explicitly include electronic forms of communication within more traditional stalking or harassment laws.

- Denial-of-Service Attacks

  In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular web site into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.

- Internet Investment Scams - SEC

  The Securities and Exchange Commission (SEC), which receives about 300 complaints a day concerning online scams, devotes one-fourth of its enforcement staff to computer-related offenses.

- Internet Scam and Hoaxes

  Email hoaxes spread misinformation, waste bandwidth, and lessen the effectiveness of email as a communication medium. Hoax-Slayer helps stop the continued circulation of these hoaxes by publishing information about them. Hoax-Slayer allows Internet users to check the veracity of a large number of common email hoaxes. Information about new hoaxes is added on a regular basis.

- National Consumers League - Online and Internet Fraud

  Our mission is to give consumers the information they need to avoid becoming victims of telemarketing and Internet fraud and to help them get their complaints to law enforcement agencies quickly and easily.

- Online Safety - Phishing

  Phishing e-mail messages are designed to steal your identity. They ask for personal data, or direct you to Web sites or phone numbers to call where they ask you to provide personal data.

a. Unauthorized access & Hacking:-

b. Trojan Attack:-

c. Virus and Worm attack:-

d. E-mail & IRC related crimes:-

1. Email spoofing

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. Please Read

2. Email Spamming

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

3 Sending malicious codes through email

E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

4. Email bombing

E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

5. Sending threatening emails

6. Defamatory emails

7. Email frauds

e. Denial of Service attacks:-

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

Examples include

attempts to "flood" a network, thereby preventing legitimate network traffic

Banking/Credit card Related crimes:-

In the corporate world, Internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information.

Use of stolen card information or fake credit/debit cards are common.

Bank employee can grab money using programs to deduce small amount of money from all customer accounts and adding it to own account also called as salami.

k. E-commerce/ Investment Frauds:-

l. Sale of illegal articles:-

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

m. Online gambling:-

There are millions of websites hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

n. Defamation: -

Defamation can be understood as the intentional infringement of another person's right to his good name.

Cyber Defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. Information posted to a bulletin board can be accessed by anyone. This means that anyone can place

Cyber defamation is also called as Cyber smearing.

---

4) E- Commerce

Electronic commerce, commonly written as **E-Commerce or eCommerce**, is the trading or facilitation of trading in products or services using computer networks, such as the Internet or online social networks.[1] Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle although it may also use other technologies such as e-mail.

E-commerce businesses may employ some or all of the following:

- Online shopping web sites for retail sales direct to consumers
- Providing or participating in online marketplaces, which process third-party business-to-consumer or consumer-to-consumer sales
- Business-to-business buying and selling
- Gathering and using demographic data through web contacts and social media
- Business-to-business electronic data interchange
- Marketing to prospective and established customers by e-mail or fax (for example, with newsletters)
- Engaging in pretail for launching new products and services

- Online financial exchanges for currency exchanges or trading purposes

5) data security

As malware attacks increase in volume and complexity, it's becoming more difficult for traditional analytic tooling and infrastructure to keep up thanks to:

- **Data volume:** For example, every day at SophosLabs, over 300,000 new potentially malicious files that require analysis are reported.
- **Scalability:** SQL-based tooling and infrastructure doesn't scale well and is costly to maintain. This Dataconomy post on SQL vs. NoSQL, What You Need to Know is a good primer on why that is and more.

Big Data Analytics as a Path Forward

The good news is companies and key analyst firms are recognizing that these challenges can be overcome with big data analytics and modern BI platforms. Analyst firms have been writing reports and advising their clients about the impacts of big data analytics on cyber security across industries:

- IDC identifies cloud and big data analytics will prevent cyber threats against health organizations
- Gartner says by 2016, 25 percent of large global companies will have adopted big data analytics for at least one security or fraud detection use case
- Ovum advises enterprises to use big data to fight security threats

So who's been there, done that, and what can you learn from them? Sophos, who began producing antivirus and encryption products nearly 30 years ago, now helps secure the networks used by 100 million people in 150 countries and 100,000 businesses using big data analytics. Today, big data analytics is integral to Sophos' daily malware detection in multiple use cases:

1. **Malware research and analysis.** Malware is becoming more evasive and pervasive. Sophos analyzes the characteristics of suspicious files and report the analysis outcome.
2. **Macro trend analysis.** Sophos analysts also analyze the data for macro trends of malware movements to better understand and anticipate the direction of the threat landscape.

3. **Measuring detection performance.** Analyzing statistics on the performance of malware detection to understand which protection technology is providing us the most value.

Threats and Opportunities

There are three main challenges that businesses are running into with big data:

- Protecting sensitive and personal information
- Data rights and ownership
- Not having the talent (i.e. data scientists) to analyze the data

While meeting the main challenge of safeguarding information may sound simple enough, when you look at the scale of data that needs to be processed and analyzed in order to prevent cyber attacks, the challenge becomes a little more daunting. For example, "to give you an idea of how much data needs to be processed, a medium–size network with 20,000 devices (laptops, smartphones and servers) will transmit more than 50 TB of data in a 24–hour period. That means that over 5 Gbits must be analyzed every second to detect cyber attacks, potential threats and malware attributed to malicious hackers," according to Computer World.

If businesses can figure out how to use modern technologies to safeguard personal and sensitive data, then the opportunities that big data present are great. The two biggest benefits big data offers companies today are:

- Business intelligence through access to vast data/customer analytics that can be used to enhance and optimize sales and marketing strategies
- Fraud detection and a SIEM systems replacement

Increasing Big Data Security

When cyber criminals target big data sets, the reward is often well worth the effort needed to penetrate security layers, which is why big data presents such a great opportunity not only for businesses but for cyber criminals. They have a lot more to gain when they go after such a large data set. Consequently, companies have a lot more to lose should they face a cyber attack without the proper security measures in place.

In order to increase the security around big data, your business may consider:

- **Collaborating with other industry peers** to create industry standards, head off government regulations, and to share best practices

- **Attribute based encryption** to protect sensitive information shared by third parties
- **Secure open source software** such as Hadoop
- **Maintain and monitor audit logs** across all facets of the business

Overall, big data presents enormous opportunities for businesses that go beyond just enhanced business intelligence. Big data offers the ability to increase cyber security itself. Yet, in order to benefit from the many opportunities big data presents, companies must shoulder the responsibility and risk of protecting that data.

---

6) Confidentiality in cyber law

Confidentiality has been defined as the "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security. Confidentiality also refers to an ethical principle associated with several professions (e.g., medicine, law, religion, professional psychology, and journalism). In ethics, and (in some places) in law and alternative forms of legal dispute resolution such as mediation, some types of communication between a person and one of these professionals are "privileged" and may not be discussed or divulged to third parties.

2. data means information which

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;

3. “processing”, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available

2. Sensitive personal data

In this Act "sensitive personal data" means personal data consisting of information as to—

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Confidentiality of Data & Various Legal Aspects:

Confidentiality involves a sense of 'expressed' or 'implied' basis of an independent equitable principle of confidence. Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Right to privacy is more of an implied obligation. It is the 'right to let alone.'

Under legal phraseology the issue of confidentiality arises where an obligation of confidence arises between a 'data collector' and a 'data subject.' This may depend upon facts & circumstances also upon the nature of information disclosed.

Discloser of confidential information may be done under any sphere; it may be in the Medical Profession, Legal Profession and discloser of security of state or military information. Sensitive Personal Data of any individual can be disclosed which may lead to his defamation or some kind of loss in his business etc. This information may be conveyed orally or in writing, it would also include information that is not in military form; i.e. Plans and ideas discussed in informal meetings between the parties. There may be 4 main classes of information covered under breach of confidence; the categories are personal information such as

material secrets.

There can be a disclosure of trade secrets also; it could be wide range of information. Technical secrets was an issue in Saltman Engineering Case & Court of Appeal upheld the existence of an equitable doctrine of confidence, independent of contract.

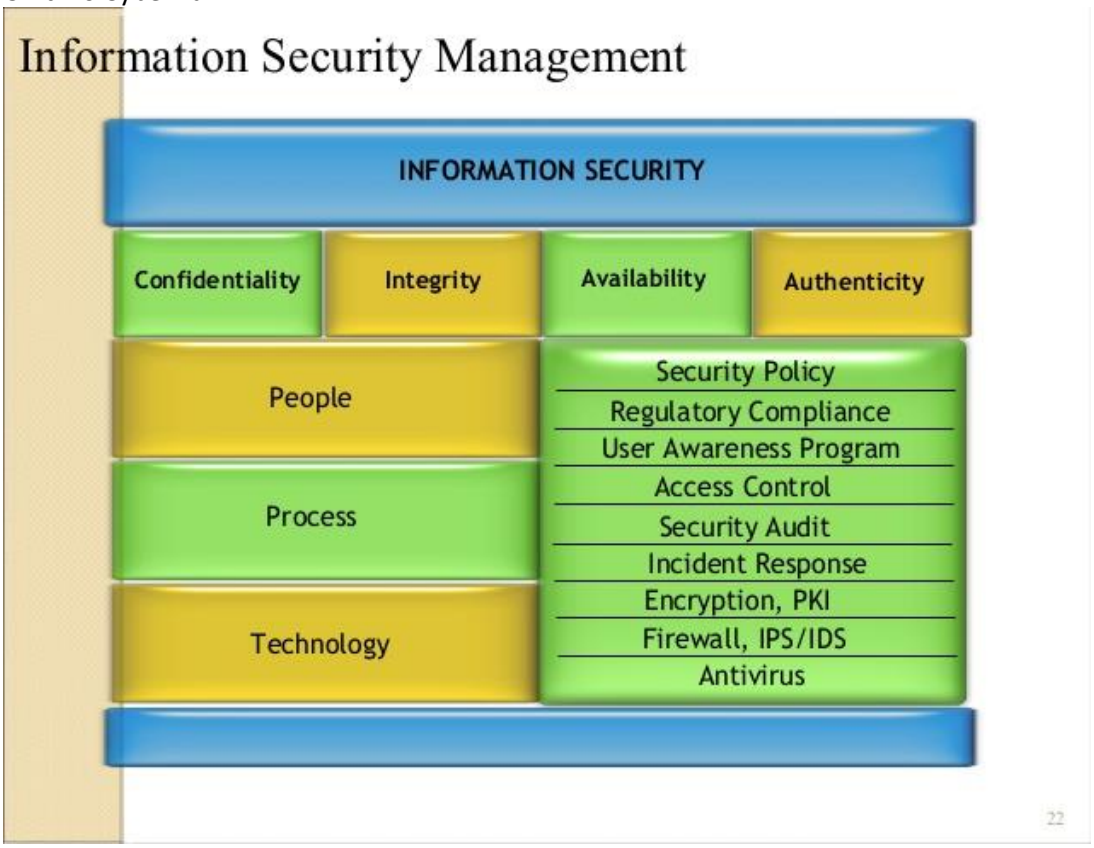
Legal Confidentiality:

Lawyers are often required by law to keep confidential anything pertaining to the representation of a client. However, most jurisdictions have exceptions for situations where the lawyer has reason to believe that the client may kill or seriously injure someone, may cause substantial injury to the financial interest or property of another, or is using (or seeking to use) the lawyer's services to perpetrate a crime or fraud.

In such situations the lawyer has the discretion, but not the obligation, to disclose information designed to prevent the planned action.

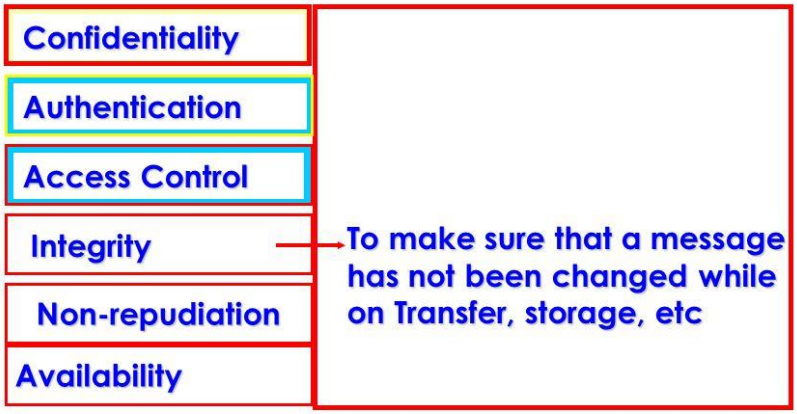
Laws Pertaining to Confidentiality of Data:

As the emergence of crimes in cyber space also the laws relating to privacy also getting firm day by day the concept of data protection is also getting its recognisition. The law does not determine what privacy is, but only what situations of privacy will be afforded legal protection. Confidentiality may be covered under law of privacy also, disclosing any one’s confidential information may be his breach of privacy.



Information Security

Security Services: Integrity



2) IT ACT 2000

The Information Technology Act, 2000

The Indian Parliament enacted an Act called the Information Technology Act, 2000. It received the assent of the President on the 9th June, 2000 and is effective from 17th October, 2000. This Act is based on the Resolution A/RES/51/162 adopted by the General Assembly of the United Nations on 30th January, 1997 regarding the Model Law on Electronic Commerce earlier adopted by the United Nations Commission on International Trade Law (UNCITRAL) in its twenty-ninth session.

The aforesaid resolution of the U.N. General Assembly recommends that all States give favourable consideration to the Model Law on Electronic Commerce when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information.

It was a foresight on the part of the Government of India to initiate the entire process of enacting India's first ever information technology legislation in the year 1997 itself.

There were three reasons:
(a) to facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions;

(b) to enable the use of digital signatures in authentication of electronic records; and

(c) to showcase India's growing IT prowess and the role of Government in safeguarding and promoting IT sector and attracting FDI in the said sector.

It is important to understand that while enacting the Information Technology Act, 2000, the legislative intent has been not to ignore the national or municipal (local) perspectives of information technology and also to ensure that it should have an

international perspective as advocated by the UNCITRAL Model Law on Electronic Commerce.

Enumeration of the main principles of the Information Technology Act, 2000

It is significant to note that by enactment of the Information Technology Act, 2000, the Indian Parliament provided a new legal idiom to data protection and privacy.

The main principles on data protection and privacy enumerated under the Information Technology Act, 2000 are:

(i) defining 'data', 'computer database', 'information', 'electronic form', 'originator', 'addressee' etc.
(ii) creating civil liability if any person accesses or secures access to computer, computer system or computer network
(iii) creating criminal liability if any person accesses or secures access to computer, computer system or computer network
(iv) declaring any computer, computer system or computer network as a protected system
(v) imposing penalty for breach of confidentiality and privacy
(vi) setting up of hierarchy of regulatory authorities, namely adjudicating officers, the Cyber Regulations Appellate Tribunal etc.

Section 72. Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance 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 other 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.

The aforesaid section has a limited application only. It confines itself to the acts and omissions of those persons, who have been conferred powers under this Act, Rules or Regulation made there under.

Section 72 of the Act relates to any person who, in pursuance of any of the

powers conferred by the Act or its allied rules and regulations has secured access to any:
i) Electronic record, ii)
book,
iii) Register,
iv) Correspondence,
v) Information,
vi) Document, or
vii) Other material.

If such person discloses such electronic record, book, register, correspondence, information, document or other material to any other person, he will be punished with imprisonment for a term, which may extend to two years, or with fine, which may extend to two years, or with fine, which may extend to one lakh rupees, or with both.

This section applies only to person who has gained access to the abovementioned information in pursuance to a power granted under Information Technology Act, its allied rules e.g. a police officer, the Controller etc. it would not apply to disclosure of personal information of a person by a website, by his email service provider etc.

Persons conferred with power under the Act
The Act has conferred powers to :
The Controller of Certifying Authorities (Ss. 17-18)
The Deputy and Assistant Controllers of Certifying Authorities (Ss. 17 and 27)
Licensed Certifying Authorities (S. 31) and Auditors (Rule 312)
The Adjudicating Officer (S 46)
The Presiding Officer of the Cyber Appellate Tribunal (Ss. 48-49)
The Registrar of the cyber Appellate tribunal (S. 56 and rule 263)
Network Service provider (S. 79)

Police Officer (Deputy Superintendent of Police) (S. 80)

The idea behind the Section 72 is that the person who has secured access to any such information shall not take unfair advantage of it by disclosing it to the third party without obtaining the consent of the disclosing party. An obligation of

confidence arises between the ‘data collectors’ and a ‘data subject’.
Instances of cyber contraventions.

The Act provides a complete Chapter (Chapter IX) on cyber contraventions, i.e., section 43 (a) – (h) which cover a wide range of cyber contraventions related to unauthorised access to computer, computer system, computer network or resources.

Section 43 of the Act covers instances such as:

(a) computer trespass, violation of privacy etc.
(b) unauthorised digital copying, downloading and extraction of data, computer database or information;. theft of data held or stored in any media,
(c) unauthorised transmission of data or programme residing within a computer, computer system or computer network (cookies, spyware, GUID or digital profiling are not legally permissible),
(d) data loss, data corruption etc.,
(e) computer data/database disruption, spamming etc.,
(f) denial of service attacks, data theft, fraud, forgery etc.,
(g) unauthorised access to computer data/computer databases and
(h) instances of data theft (passwords, login IDs) etc.

The Information Technology Act, 2000 provides for civil liability in case of data, computer database theft, privacy violation etc.
The Act also provides a complete Chapter (Chapter XI) on cyber offences, i.e., sections 65-74 which cover a wide range of cyber offences, including offences related to unauthorised alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, and computer database.

For example, section 65 [Tampering with computer source documents] of the Act is not limited to protecting computer source code only, but it also safeguards data and computer databases; and similarly section 66 [Hacking with Computer System] covers cyber offences related to (a) Illegal access, (b) Illegal interception, (c) Data interference, (d) System interference, (e) Misuse of devices, etc.

The Information Technology Act, 2000 provides for criminal liability in case of data, computer database theft, privacy violation etc.

Proposed amendments to the Information Technology Act, 2000 vis-à-vis data protection and privacy

The Expert Panel constituted by the Department of Information Technology, Ministry of Information Technology, Government of India in its recommendations4 proposed following amendments in the Act to strengthen data protection and privacy:

Section 43, Explanation

(v) "Reasonable security practices and procedures" means, in the absence of a contract between the parties or any special law for this purpose, such security practices and procedures as appropriate to the nature of the information to protect that information from unauthorized access, damage, use, modification, disclosure or impairment, as may be prescribed by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

Section 43, Explanation (vi) "Sensitive personal data or information" means such personal information, which is prescribed as "sensitive" by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

It is obligatory to note that not only the aforementioned proposed amendments would pave the way of self-regulation in terms of defining what constitute: "reasonable security practices and procedures" and "sensitive personal data or information" but also grant statutory protection to sensitive personal data. Further, the proposed amendments have enlarged the scope of section 66 by making it consistent with the provisions of the Indian Penal Code, 1860, and also providing extent of criminal liabilities in case of data, computer database theft, privacy violation etc. Moreover, newly proposed sub-section (2) of section 72 makes the intermediaries (network service providers) liable for data and privacy violations. Now, such intermediaries to pay damages by way of compensation to the subscriber so affected.

The Information Technology Act, 2000 and Privacy Protection: A Critique

The Information Technology Act, 2000 is not data or privacy protection legislation per se. It does not lay down any specific data protection or

privacy principles. The Information Technology Act, 2000 is a generic legislation, which articulates on range of themes, like digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offences and confidentiality and privacy. It suffers from a one Act syndrome.

In fact the Information Technology Act, 2000 deals with the issue of data protection and privacy in a piecemeal fashion. There is no an actual legal framework in the form of Data Protection Authority, data quality and proportionality, data transparency etc. which properly addresses and covers data protection issues. Even if the new proposed amendments to the Information Technology Act, 2000 were adopted, India would still lack a real legal framework for data protection and privacy

---

7) PRIVACY IN CYBER LAW

The use of the Internet can affect the privacy rights a person has in his or her identity or personal data. Internet use and transactions generate a large amount of personal information which provide insights into your personality and interests.

Privacy issues relating to **identity** include the possible appropriation of a person's email identity and address.

- Ease of access to and the appropriation of email addresses has led to the practice of sending vast amounts of unsolicited e-mails (spam).

Identification through email and website transactions and the ability to locate people's physical addresses easily through national and international directories have raised new privacy concerns.

Privacy issues relating to **personal data** arise from

- insecure electronic transmissions,
- data trails and logs of email messages,
- online transactions and the
- tracking of web pages visited.

Privacy invasion issues arise from **data matching** (the process of wholesale cross checking of data from one source against another source such as tax and social security data) and personal profile extraction processes which use this data alone or in combination with other publicly available data.

The first half of Roger Clarke's article Introducing PITs and PETs: Technologies Affecting Privacy1 [1] also highlights some of the privacy concerns arising from the Internet and technology generally.

The regulators: Privacy Commissioners

Where?

- federally (http://www.privacy.gov.au), in
- NSW (http://www.lawlink.nsw.gov.au/pc.nsf/pages/index) and
- Victoria (http://www.privacy.vic.gov.au),
- but currently not in other states.
-

Privacy Commissioners have certain responsibilities under relevant Commonwealth and State privacy legislation. Their **functions** include:

- handling complaints by individuals who feel their privacy rights may have been breached;
- assisting governments and private sector bodies (where applicable) comply with relevant privacy legislation;
- providing information advice to the public about their privacy rights; and
- policy development.

Public sector Commonwealth legislation

Personal information under s 6 of the *Privacy Act* is defined as:

- **credit providers and credit-reporting agencies** must comply with credit reporting rules in the Act and in the legally binding code of conduct dealing with credit rating information of individuals;

- **all organisations that store and use tax file number information** must comply with tax file number guidelines issued by the Privacy Commissioner (s 17 *Privacy Act*).

The NPPs deal with the same main issues as the IPPs:

- collection,
- use,
- disclosure,
- storage and
- security of information and
- rights to access this information.

The Privacy Commissioner has the power to:

- investigate a complaint made to the Privacy Commissioner;
- investigate a complaint that a code adjudicator has referred to the Privacy Commissioner;
- to hear appeals from a decision of a code adjudicator;
- investigate all complaints made about a federal Government contractor;
- investigate an act or practice that may be a breach of privacy (even if no complaint has been made);
- seek an injunction from the Federal Court to restrain or prohibit a person from engaging in conduct that does or would breaching the *Privacy Act*. No undertaking as to damages is required if application is made by the Commissioner.
