The new world of information society with global networks and cyberspace will inevitably generate a wide variety of social, political, and ethical problems. Many problems related to human relationships and the communities become apparent, when most human activities are carried on in cyberspace. Using the library-based methodology, the study focuses on the ethical issues in information technology. Based on extant literature, several ethical issues such as plagiarism, hacking, viruses, data access rights, piracy, ergonomy and health issues amongst others were identified as possible ethical issues related to IT. These basic issues have been solved partially using technological approaches, such as encryption technique, SSL, digital IDs and computer firewalls. Besides these protection technologies, legal laws are also needed in cyberspace to address hundreds of countries, which are incorporated into one global network. Guidelines and strategies should be implemented so that global information can be exploited in a socially and ethically sensitive way for our future benefit and applications.

1. **INTRODUCTION THE CONCEPT OF ETHICS THEORY**

The notion of ethics is regularly drawn upon in the context of expected patterns of behaviors written or unwritten, consistent with generally accepted standards for those to whom it may concern. However, there are various perspectives on the concept of ethics. Griffin cited in Agbonifoh (2002) defines the concept as an individual’s personal belief about what is right or wrong, good or bad. Conversely, Miner (2002) defined ethics as right or wrong actions that stems from the value and expectation of society. Mintz and Morris (2007) notes that ethics are acceptable standards of behaviour that define how people ought to act (i.e. prescriptive) not how people really act (i.e. descriptive). Nevertheless, the generic sociological meaning of the concept of ethics seems to provide a common ground for most of them. Sociologically speaking, ethics are provided in order to render behavior intelligible and to “prevent conflicts from arising by bridging the gap between action and expectation” (Scott & Lyman, 1968).

In the context of an operational definition with regards to professions, Ethics generally refers to those principles and codes of behaviour that guide the conduct of any profession. The term usually carries along moral values, normative judgments and moral obligations. At any rate, every profession possesses its own ethics. However, there are some commonalities in professional ethics. These ethics that are common derive from the general expectations of the public from either a public officer or a professional practitioner. The issue of ethics usually goes along with allocation of value judgment such as good or bad; right or wrong. Fisher (2004) defines the concept as an individual’s personal belief about what is right or wrong, good or bad. It is the arbiter of an individual’s evaluation of the “rightness” or otherwise of his or her actions. Though often regarded as subjective, it is traceable to the foundation of an individual’s belief system and judged within context. Conversely, Logsdon and Yuthas (1997) notes that the ethical stance of a firm is constructed based on the expectation of society, that is, the legitimate claims made by the constituencies to whom the firm interacts. According to Hanekom (1984), the question of ethics is one that is linked with the history of mankind. Ethics deals with the character and conduct and morals of human beings. It deals with good or bad, right or wrong behaviour. It evaluates conduct against some absolute criteria and puts negative orpositive values on it. It is the reflective study of what one ought to do, or how one ought to live. Erondu, Sharland and Okpara (2004) hold that the study of “ethics” focuses on issues of practical decision making, including the nature of ultimate value, and standards by which a human action can be judged right or wrong, good or bad. For Adenubi (1999), ethics applies to any system or theory of moral values or principles. For Beauchamp and Bowie (2001), ethics is the general term referring to both moral beliefs and ethical theory on human conduct Ethics is a reflection on morality. It refers to the principles of right and wrong in making choices by individuals. It has been described as the art and science that seeks to bring sensitivity and methods to the discernment of moral values (Carbo, 2006). Thus, ethics guide human and societal behavior. Capuro (2006) had no difficulty in asserting that ethics is an unending quest on explicit and implicit use of the moral code. It can also be describe as the rules of conduct or moral principles that are recognised in respect to a particular class of human action or a particular group, culture, profession. Rue and Byars (2000) are of the views that ethics are principles of conduct used to govern the decision-making and behaviour of an individual or a group of individuals. They further indicate that because management is concerned with making decisions within an organization, the ethics of the individual or group making these decisions have significant implications for the organization’s stakeholders: employees, customers, shareholders, suppliers, the government, and the public at large.

According to Cyert and March (1992) Ethics and morals are synonymous. Ethics is derived from Greek while morals are derived from Latin. They are identical terms referring to ideals of character and conduct. These ideals, in the form of codes of conduct become the criteria for distinguishing between right and wrong”. Ethics is therefore the same thing as morality and they shape our conduct and behaviour right from childhood through adolescence and adulthood. In every aspect of life our conduct and behaviour is guided by what we were taught to be right or wrong. Heynes (1986) is of the opinion that ethics has to do with the actions of man. Consequently, it requires adjustments in the actions and attitudes of the individual in whatever context in relation to his environment as well as in relation to himself. He notes that ethics are basic perceptions of the relative importance of our elements of existence. These perceptions always have to do with priorities, whereas norms are the function by which direct evaluation of human attitudes and actions is made possible

**2.0. PHILOSOPHICAL THEORIES OF ETHICS**

**2.1. Ethical theories**

**Utilitarianism**

Two British philosophers, Jeremy Bentham and John Stuart Mill, developed utilitarianism as an ethical model in the early 1800’s. Utilitarianism is a consequence based theory, stating that the only real factor a person should consider when making a decision is the consequence of the action and the number of people positively affected. The right (or good) choice is the one that provides the best outcome for the majority of people. At the basic level, this theory has the decision maker focusing on the consequences of his decision, looking for the best solution for all affected parties. Human nature makes it difficult to determine what choice provides the most positive benefit. There is no universal scale with which to measure the utility of a decision with regard to its overall effects. It is easy for consequence-based decisions to become situational, with the decision maker rationalizing actions for a self-serving purpose. Focusing on the consequences of a decision first does not necessarily create situations that are conducive to choosing the most ethical path when the less ethical path can be reasoned to be the better choice in general.

**Pluralism**

Resnik (2010) notes that as a theory based in doing one’s duty, pluralism holds that decisions should be made out of a sense of duty to do the right thing. According to this ethical theory, as rational beings, humans are able to resist impulse and do the right thing absolutely, regardless of the consequences. The concept of duty within this theory is that of doing the right thing with the right attitude for the right reason. Proponents of this theory espouse that the duty to do the “right” thing is absolute, without exception, regardless of circumstance. This is where the opponents of this theory take issue. Nothing can be considered absolute in the arena of personal human interaction because of the innumerable variables involved. The models above illustrate the very basics of ethics and ethical theory.

**Justice**

Generally, justics is as fairness, which refers to the correlation between contribution and reward. However, fairness alone cannot define the term justice (according to R.A. ANISEREHAMEED & F.M AJIDE) Ethics in accounting, there are also forms of justice, which includes equality (assumes that all people have equal worth), procedural justice (concerns with due process) and compensatory justics (addresses the loss from a wrongful act).

Theory of justice, which is based on the principles of distributive justics, it focuses on how fairly one’s decisions distribute benefits and burdens amongst members of the group. Unjust distribution of benefits and burdens is an unjust act and an unjust act is a morally wrong act. Hence, under this theory, an ethical decision is one that produces the fairest overall distribution of benefits and burdens

1. **Ethical Issues in Information Technology**

Before now, business success was built on the ability to move goods and services with speed and accuracy. Today, information has become the fuel that propels business success. Information technology has been defined as the processing and distribution of data using computer hardware, software, telecommunications and digital electronics. . As noted by Carbo (2006) ethical considerations for ICT related issues first appeared under the topic ‘’information ethics’’ in the Annual Review of Information Science and Technology in 1992. This suggests that there is an ethical agenda associated with the use of ICT. Individuals and organisations therefore need to be ethically sensitive as they deploy ICT on their operations. The impact of ICT on human relationship has been tremendous. ICT has helped to enhance family relationship (e.g. mobile phones, palmtops, laptops, virtual conferencing and so on), as well help to separate family and friends from each other. ICT has enabled new friendship

and relationships in virtual communities. How genuine are such relationship? What does it portend for individual satisfaction? In the workplace for instance, new kinds of jobs are being created such as data miners, web-counselors etc, but these opportunities are also endangered by problems of unemployment from computer replacing humans. A wide range of new laws, regulations, rules and practices are therefore needed if society is to manage these workplace and other changes and development brought about by ICT. Thus the society need to consider the following ethical and social challenges related to ICT use:

➢ Recognition for personal and corporate ethics associated with ICT.

➢ Striking a balance between ethical, economic and technological (Rogerson, 2008) as well as political considerations.

1. Intellectual property rights issue (trademarks, patents, copyright and trade secrets).

2. Non violation of privacy and associated rights amidst electronic information data mining.

3. The opportunity to commit crime with ICT (computer crime).

4. Legal issues and limitations. 5. Consequence of using ICT.

6. Professional responsibilities (Kallman and Grillo, 1999)

**4.0. CONCEPTS OF ETHICAL ISSUES**

In the rapidly changing technological environment in which we live; ethical issues are increasingly been raised, demanding attention and efforts towards resolution. Of particular interest for us and the information society are those related to information communication technologies (ICTs). The explosive growth of ICT and the use of its enabling technologies have had major impacts on society and thus raise serious ethical questions for individuals and organisations. These issues have been raised to a new and often perplexing level which has greatly affected the society in various ways. The pressing issues raised by ICT include the invasion of individual and corporate privacy, intellectual property rights, individual and societal rights, values preservation and accountability for the consequences arising from the use of ICT, etc.These issues have thrown up important challenges in the area of employment; working conditions and individuality. However, not much progress has been made in addressing these issues and challenges associated with ICT.

According to Fielden, (2004), Information Technology (IT) has a central role in commerce, industry, government, medicine, education, entertainment and society at large. Its economic and social benefits hardly need explanation. But like any other technologies, IT also has problematic implications, and some negative impacts on our society. It poses and creates some problems related to ethics, and contains in general three main types of ethical issues: personal privacy, access right, and harmful actions. In terms of personal privacy, IT enables data exchange of information on a large scale from anybody, on any locations or parts of the world, at any times. In this situation, there is increased potential for disclosing information and violating the privacy of any individuals and groups of people due to its widespread disseminations worldwide. It is our challenge and responsibility to maintain the privacy and integrity of data regarding individuals. This also includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals.

The second aspect of ethical issues in computing systems is access right. Due to the current popularity of international commerce on the Internet, the topic of computer security and access right has moved quickly from being a low priority for corporations and government agencies to a high priority. This interest has been heightened by computer breakins at places like Los Alamos National Laboratories and NASA in the US. Many attempts of such illegal access to United States government and military computers by computer hackers have been widely reported. Without implementation of proper computer security policies and strategies, network connections on the Internet can’t be made secure from illegal accesses (Grimesm Fleischman & Jaeger 2009).

Grimes, Fleischman & Jaeger (2009) notes that in computer ethics, harmful action means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of users, the general public, employees, and employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems from "computer viruses. We shall also examine other specific ethical issues arising from IT below;

**4.1. Plagiarism**

Plagiarism is where the work of others is copied, but the author presents it as his or her own work. This is a highly unethical practice, but happens quite frequently, and with all the information that is now available on the Internet it is much easier to do and is happening more often

**Information and copyright**

**Education**

Commerce and industry are certainly arenas in which the Internet has had a profound effect, but what of the foundational institutions of any society—namely, those related to education and the production of knowledge? Here the Internet has had a variety of effects, some of which are quite disturbing. There are more computers in the classroom than ever before, but there is scant evidence that they enhance the learning of basic skills in reading, writing, and arithmetic. And while access to vast amounts of digital information is convenient, it has also become apparent that most students now see libraries as antiquated institutions better used for their computer terminals than for their book collections. As teachers at all education levels can attest, students typically prefer to research their papers by reading online rather than wandering through a library's stacks.

In a related effect the Internet has brought plagiarism into the computer era in two distinct senses. First, electronic texts have made it simple for students to “cut and paste” published sources (e.g., encyclopaedia articles) into their own papers. Second, although students could always get someone to write their papers for them, it is now much easier to find and purchase anonymous papers at Web sites and to even commission original term papers for a fixed fee. Ironically, what the Internet gives, it also takes away. Teachers now have access to databases of electronically submitted papers and can easily compare their own students' papers against a vast archive of sources. Even a simple online search can sometimes find where one particularly well-turned phrase originally appeared.

**Piracy**

Piracy, the illegal copying of software, is a very serious problem, and it is estimated that approximately 50% of all programs on PCs are pirated copies. Programmers spend hours and hours designing programs, using elaborate code, and surely need to be protected. Although some might argue that some pirating at least should be permitted as it can help to lead to a more computer literate population. But, for corporations, in particular, this is a very serious issue, and can significantly damage profit margins (White 2002).

**File Sharing**

College students have been at the leading edge of the growing awareness of the centrality of intellectual property in a digital age. When American college student Shawn Fanning invented Napster in 1999, he set in motion an ongoing legal battle over digital rights. Napster was a file-sharing system that allowed users to share electronic copies of music online. The problem was obvious: recording companies were losing revenues as one legal copy of a song was shared among many people. Although the record companies succeeded in shutting down Napster, they found themselves having to contend with a new form of file sharing, P2P (“person-to-person”). In P2P there is no central administrator to shut down as there had been with Napster. Initially, the recording industry sued the makers of P2P software and a few of the most prolific users—often

students located on university campuses with access to highspeed connections for serving music and, later, movie files—in an attempt to discourage the millions of people who regularly used the software. Still, even while some P2P software makers have been held liable for losses that the copyright owners have incurred, more-devious schemes for circumventing apprehension have been invented. The inability to prevent file sharing has led the recording and movie industries to devise sophisticated copy protection on their CDs and DVDs. In a particularly controversial incident, Sony Corporation introduced CDs into the market in 2005 with copy protection that involved a special viruslike code that hid on a user's computer. This code, however, also was open to being exploited by virus writers to gain control of users' machines.

**Hacking**

A hacker is an individual who is knowledgeable enough to gain access without authorization to computer systems to identify security flaws. Hackers break into, or ‘hack’ into a system. Hacking can be undertaken for a variety of reasons, such as the wish to damage a system or the wish to understand how a system works, so that money can be made out of it. Alternatively, there might be a desire to alert people to the fact that a system is insecure and needs improving. Due to this some argue that there are ‘hacker ethics’. Hacking can present a moral dilemma. This is because ‘reformed hackers’ sometimes offer their expertise to help organisations protect themselves against other hackers. Hackers cannot just wander into a system, as they could into an unlocked door. Instead, it requires a lot of skill. With this skill hackers can demonstrate that a system is insecure and needs improving. In this way, it could be argued that hackers play a valuable role. Many argue that hacking might lead to some improvements, but that it causes such a lot of disruption that it is not worth it in the long-run (McCarthy, Halawi ., Aronson, 2005)

**Computer Crime**

By some estimates the personal records of about 73 million people in the U.S. were accidentally disclosed, lost, or stolen in 2006. In one high-profile case, a burglary at the home of an employee of the U.S. Department of Veterans Affairs resulted in the theft of a computer that contained personal data on more than 26 million current and former members of the U.S. military. The computer was later recovered, its data apparently untouched by the thieves, who had not realized what they had taken. There were fears that millions of other people might not be so lucky, however. In many cases the lost information included credit-card and Social Security numbers, which fueled concerns that stolen information could lead to widespread consumer fraud. In an 18-month period during 2005–06, well over 200 different security breaches at companies and government agencies were reported. As a result, credit-card issuers tried to reduce their vulnerability by pressuring companies that handled credit-card transactions to comply with strict new credit-card security standards that were backed by Visa and MasterCard. As the year ended, it appeared that identity theft had not risen to the level suggested by the amount of personal information that had been compromised, but there was no way to know whether identity thieves were simply biding their time before they used the information to steal money through bank or credit-card accounts.

Perpetrators of identity theft who had been caught recounted the ease with which they cashed in on stolen information. Thieves typically stole identity information when it was inadvertently disclosed or through “phishing” schemes, in which they used e-mail to persuade people to submit a creditcard number or other personal information to a fake Web page that pretended to represent a real business. Using a stolen credit-card number, the thieves then transferred money to themselves from a victim's account or purchased goods by using the victim's identity. The scope of the theft efforts was huge; in a single month more than 17,000 phishing attacks were reported to volunteer groups trying to prevent identity theft.

Many different computer crimes are committed, which clearly poses ethical questions for society. Various illegal acts are performed on computers, such as fraud and embezzlement. This includes, for example, using imaging and desktop publishing to create, copy or alter official documents and graphic images. There are also various ethical dilemmas, such as whether copying such files is as bad as stealing something.

**Malicious Code**

Malicious code attacks include a number of types of computer programs that were created with the intention of causing data loss or damage. The three main types of malicious code attacks are viruses, Trojan horses, and worms. A virus is malicious software that is attached to another program to execute a particular unwanted function on a workstation. An example is a program that is attached to command.com (the primary interpreter for Windows systems) and deletes certain files and infects any other versions of command.com that it can find. A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on a workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every address in the user's address book. The other users receive the game and play it, thereby spreading the Trojan horse to the addresses in each address book.

Viruses normally require a delivery mechanism, a vector, such as a zip file or some other executable file attached to an email, to carry the virus code from one system to another. The key element that distinguishes a computer worm from a computer virus is that human interaction is required to facilitate the spread of a virus. Worms are self-contained programs that attack a system and try to exploit a specific vulnerability in the target. Upon successful exploitation of the vulnerability, the worm copies its program from the attacking host to the newly exploited system to begin the cycle again A virus consists of a set of instructions that attaches itself to other computer programs, usually in the computer's operating system, and becomes part of them. In most cases, the corrupted programs continue to perform their intended functions but surreptitiously execute the virus's instructions as well. A virus is usually designed to execute when it is loaded into a computer's memory. Upon execution, the virus instructs its host program to copy the viral code into, or “infect,” any number of other programs and files stored in the computer. The infection can then transfer itself to files and code on other computers through magnetic disks or other memory-storage devices, computer networks, or online systems. The replicating viruses often multiply until they destroy data or render other program codes meaningless. A virus may simply cause a harmless joke or cryptic message to appear on a computer user's video monitor each time he turns on his computer. A more damaging virus can wreak havoc on an extremely large computer system within a matter of minutes or hours, causing it to crash and thereby destroy valuable data. Clearly writing and spreading virus programs are unethical acts; they have very serious consequences, and cause systems to crash and organisations to cease operating for certain periods. One of the most concerning consequences of such actions is when viruses interrupt the smooth functioning of an organisation which could in extreme cases even cause people to die. Logic bombs are also sometimes planted. There is obviously a lot of anti-virus software on the market now though that helps to deal with this ever-growing problem.

**Ergonomics/Health Issues**

There are many ergonomic/health issues related to I.T. Responsible/ethically-minded employers will, hopefully, give due consideration to this, as indeed should all employers. This includes issues such as the importance of taking adequate breaks from using the computer and ensuring that the screens comply with the regulations. Also, ensuring that the positioning of the chair and the computer is appropriate for the user and providing foot rests, when required. Some organisations will give special advice to their employees on these matters. Without such ethical/moral awareness and taking the necessary action, many workers will suffer health problems directly from I.T., such as back problems, eyestrain and eye infections and repetitive strain injury (RSI).

**Job displacement/work pressures imposed on computer professionals**

Computers are changing the face of the work scene. For some people, their jobs are becoming redundant or they have to play quite different roles, and others are suffering increasing levels of stress from work pressures. Others are, obviously, reaping the benefits of having more rewarding jobs, and there is certainly more emphasis on knowledge, information and I.T. skills than ever before. However, this all clearly poses various ethical issues. Should those that lose their jobs be compensated? How can the pressure be eased on those that are suffering stress? Is it acceptable for computer programmers to be made redundant ‘on the spot’ etc? There are many ethical issues that need to be addressed here

**Digital Divide**

The digital divide poses a serious problem today. A new breed of haves’ and ‘have nots’ are being created, between those that have access and can use a computer and the Internet, and those that do not have such access. There are clearly serious ethical implications here. Those that do not have such access may well be discriminated against, feel ‘socially excluded’ and miss out on many life opportunities

**5. International Efforts on Legislations**

According to Bessen and Hunt (2004), the growing threat to individuals is beginning to claim attention in national and international community. In many countries around the world, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would pose false information, from who steal, deny access to, or even destroy valuable information. Self-protection is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cybercrime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current statutes to determine whether they are sufficient to combat such kinds of crimes. Until now, only few nations have amended their laws to cover computer crimes that need to be addressed, as shown in Table 3. Other countries begin to implement some initiatives, and it is clear that a great deal of additional work and efforts are needed before organizations and individuals can be confident that cyber criminals will think twice before attacking valued systems and information

**Computer/Cyber Fraud:**

The term fraud may be defined as the intentional misrepresentation of financial information by one or more individual among management, employees or third parties. The use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

**Defining Cybercrime**

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the “cyber” prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities. Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity. An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified. In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Cybercrime Convention was signed by 30 states. Additional protocols, covering terrorist activities and racist and xenophobic cybercrimes were proposed in 2002. In addition, various national laws, such as the USA PATRIOT Act of 2001, have expanded law enforcement's power to monitor and protect computer networks

**Types of cybercrimes**

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual. Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another part of this type of crime involves individuals within corporations or government bureaucracies deliberately altering data for either profit or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These range from spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism— that is, the use of the Internet to cause public disturbances and even death. Cyberterrorism focuses upon the use of the Internet by nonstate actors to affect a nation's economic and technological infrastructure. Since the September 11 attacks of 2001, public awareness of the threat of cyberterrorism has grown dramatically.

**Identity theft and invasion of privacy**

richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified. In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Cybercrime Convention was signed by 30 states. Additional protocols, covering terrorist activities and racist and xenophobic cybercrimes were proposed in 2002. In addition, various national laws, such as the USA PATRIOT Act of 2001, have expanded law enforcement's power to monitor and protect computer networks

Security card; it is then possible to open bank accounts and receive loans—all with the victim's credit record and background. The original cardholder might remain unaware of this until the debt is so great that the bank contacts the account holder. Only then does the identity theft become visible. Although identity theft takes places in many countries, researchers and law-enforcement officials are plagued by a lack of information and statistics about the crime worldwide. Interpol, the international policing agency, has not added any type of cybercrime, including identity theft, to its annual crime statistics. Cybercrime is clearly, however, an international problem. In 2003 the U.S. Federal Trade Commission released the first national survey on identity theft; according to the report, in the previous year 3.3 million Americans had their identities fraudulently used to open bank, credit card, or utility accounts, with losses of $32.9 billion to businesses and $3.8 billion to individuals. The report also stated that 6.6 million Americans were victimized by account theft, such as use of stolen credit cards and automatic teller machine (ATM) cards, with losses of $14 billion to businesses and $1.1 billion to individuals.

**Internet Fraud**

Schemes to defraud consumers abound on the Internet. Among the most famous is the Nigerian, or “419,” scam; the number is a reference to the section of Nigerian law that the scam violates. Although this con has been used with both fax and traditional mail, it has been given new life by the Internet. In the scheme, an individual receives an e-mail asserting that the sender requires help in transferring a large sum of money out of Nigeria or another distant country. Usually, this money is in the form of an asset that is going to be sold, such as oil, or a large amount of cash that requires “laundering” to conceal its source; the variations are endless, and new specifics are constantly being developed. The message asks the recipient to cover some cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future. Should the recipient respond with a check or money order, he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable. In 2002 the U.S. Internet Fraud Complaint Center reported that more than $54 million dollars had been lost through a variety of fraud schemes; this represented a threefold increase over estimated losses of $17 million in 2001. In the United States, the largest source of fraud was online auctions. In many cases, individuals would put products up for sale on Internet auction sites, demand money before delivery, and never fulfill their obligations to the consumer. Such scams accounted for 46 percent of the fraud cases in 2002, with an average individual loss of $299. Unlike identity theft, where the theft occurs without the victim's knowledge, these more traditional forms of fraud occur in plain sight. The victim willingly provides private information that enables the crime; hence, these are transactional crimes. Few people would believe someone who walked up to them on the street and promised them easy riches; however, receiving an unsolicited e-mail or visiting a random Web page is sufficiently different that many people easily open their wallets. Despite a vast amount of consumer education, Internet fraud remains a growth industry for criminals and prosecutors. Europe and the United States are far from the only sites of cybercrime. South Korea is among the most wired countries in the world, and its cybercrime fraud statistics are growing at an alarming rate. In 2003 some 40,000 cases of cybercriminal activity, mostly fraud, had been reported to authorities. This represented an 18 percent increase from 2002. Japan has also experienced a rapid growth in similar crimes; in 2003 official National Police Agency statistics cited a 94 percent increase in Internet fraud since 2000.

**ATM Fraud**

Computers also make more mundane types of fraud possible. Take the automated teller machine (ATM) through which many people now get cash. In order to access an account, a user supplies a card and personal identification number (PIN). Criminals have developed means to intercept both the data on the card's magnetic strip as well as the user's PIN. In turn, the information is used to create fake cards that are then used to withdraw funds from the unsuspecting individual's account. In 1999 there were 251 reported cases of ATM fraud in the United States; in 2002 the New York Times reported that more than 21,000 American bank accounts had been skimmed by a single group engaged in acquiring ATM information illegally. A particularly effective form of fraud has involved the use of ATMs in shopping centres and convenience stores. These machines are free-standing and not physically part of a bank. Criminals can easily set up a machine that looks like a legitimate machine; instead of dispensing money, however, the machine gathers information on users and only tells them that the machine is out of order after they have typed in their PINs. Given that ATMs are the preferred method for dispensing currency all over the world, ATM fraud has become an international problem with multiple solutions. In August 2003 an individual in Australia pleaded guilty to stealing $A 623,000 from bank customers by using a small camera and an electronic recording device at multiple ATMs. Australia is now considering a ban on the purchase of equipment that criminals might use in ATMs to defraud customers. However, the range of equipment under consideration is quite large and useful for a variety of legitimate purposes as well.

**File Sharing and Privacy**

Sales of compact discs (CDs) are the major source of revenue for recording companies. Although piracy—that is, the illegal duplication of copyrighted materials—has always been a problem, especially in the Far East, the proliferation on college campuses of inexpensive personal computers capable of capturing music off CDs and sharing them over high-speed (“broadband”) Internet connections has become the recording industry's greatest nightmare. In the United States, the recording industry, represented by the Recording Industry Association of America (RIAA), attacked a single file-sharing service, Napster, which from 1999 to 2001 allowed users across the Internet access to music files, stored in the datacompression format known as MP3, on other users' computers by way of Napster's central computer. According to the RIAA, Napster users regularly violated the copyright of recording artists, and the service had to stop. For users, the issues were not so clear-cut. At the core of the Napster case was the issue of fair use. Individuals who had purchased a CD were clearly allowed to listen to the music, whether in their home stereo, automobile sound system, or personal computer. What they did not have the right to do, argued the RIAA, was to make the CD available to thousands of others who could make a perfect digital copy of the music and create their own CDs. Users rejoined that sharing their files was a fair use of copyrighted material for which they had paid a fair price. In the end, the RIAA argued that a whole new class of cybercriminal had been born—the digital pirate—that included just about anyone who had ever shared or downloaded an MP3 file. Although the RIAA successfully shuttered Napster, a new type of file-sharing service, known as peer-to-peer (P2P) networks, sprang up.

These decentralized systems do not rely on a central facilitating computer; instead, they consist of millions of users who voluntarily open their own computers to others for file sharing. The RIAA continues to battle these file-sharing networks, demanding that ISPs turn over records of their customers who move large quantities of data over their networks, but the effects have been minimal. The RIAA's other tactic has been to push for the development of technologies to enforce the digital rights of copyright holders. So-called digital rights management technology is an attempt to forestall piracy through technologies that will not allow consumers to share files or possess “too many” copies of a copyrighted work. As companies work on the hardware and software necessary to meet these goals, it is clear that file sharing has brought about a fundamental reconstruction of the relationship between producers, distributors, and consumers of artistic material. As broadband Internet connections proliferate, the motion-picture industry faces a similar problem, although the digital videodisc (DVD) came to market with encryption and various built-in attempts to avoid the problems of a video Napster.

**Child Pornography**

With the advent of almost every new media technology, pornography has been its “killer app,” or the application that drove early deployment of technical innovations in search of profit. The Internet was no exception, but there is a criminal element to this business bonanza—child pornography, which is unrelated to the lucrative business of legal adult-oriented pornography. The possession of child pornography, defined here as images of children under age 18 engaged in sexual behaviour, is illegal in the United States, the European Union, and many other countries, but it remains a problem that has no easy solution. The problem is compounded by the ability of “kiddie porn” Web sites to disseminate their material from locations, such as states of the former Soviet Union as well as Southeast Asia, that lack cybercrime laws. Some lawenforcement organizations believe that child pornography represents a $3-billion-a-year industry and that more than 10,000 Internet locations provide access to these materials.

**ETHICAL CHANLLENGES ON INFORMATION TECHNOLOGY**

As much as information technology is important to our lives, it is facing some serious ethical challenges, and it is up to the IT experts and users of information technology to be ready for these challenges. As more emerging information technologies pop up on the market, most of the IT experts and users do not know how to go about the challenges brought by these technologies. Information technology is facing one of its biggest challenges which are lack of privacy, security, copyright infringement and increased computer crimes. This has stimulated criminals to exploit users of IT basing on the lope holes left in these technologies. Since information technology speeds the access and flow of information, many businesses and organizations are at risk of losing this data because experienced criminals can easily tap that information for their personal use. Also unfaithful employees can use information technology to archive their personal goals which might be harmful to an organization. IT is not bad by its self, but the way humans use the tools provided by information technology has brought some serious challenges.

Below are some issues on Ethical Challenges of Information Technology

* **Security:**

With tools like the internet, hackers have found it very easy to hack into any computer or system as long as it is connected on internet. Hackers can easily use an IP (Internet Protocol) address to access a user’s computer and collect data for selfish reasons. Also the wide spread of internet cookies which collect information whenever we use the internet , has exposed IT users to high risks of fraud and conflicting interests. Many big companies use these cookies to determine which products or service they can advertise to us. When it comes to online banking, the transfer of money can easily be interrupted by a hacker and all the money will be transferred to their desired accounts , which affects both the bank and the customers who is using online banking technology.

* **Copyright Infringement:**

Information technology has made it easy for users to access any information or artifact at any given time. With the increased development of music sharing networks and photo bookmarking sites, many original creators of these works are losing the credibility of their works, because users of IT can easily gain access and share that data with friends. Free music and file downloading sites are popping up on internet every day , lots of original work like music albums, books , are being downloaded for free. In this case one legitimate user will purchase the book , software, web template or music album, and they will submit it to a free download site where others will simply just download that data for free. It is good news for the users because it saves them money, but it harms the original creator of these works. The government has closed some of these sites likeMEGAUPLOAD.COM , but many are popping up using funny URLs.

* **Increased pressure on IT experts.**

Since information technology systems have to run all the time, pressure is mounted on IT experts to ensure the accuracy and availability of these systems. Many big organizations which need to operate 24 hours will require a standby IT team to cater for any issues which might arise during the course of operation. This pressure results into stress and work overload which some times results into Imperfection.

* **Digital divide:**

Information technology has many opportunities and it has shaped many industries in developed countries; however, developing countries have difficulties of enjoying the same benefits of Information technology. To get these benefits they have to train their labor and users should also adopt the new culture which is a bit costly in these developing countries. In some remote areas they do not even have power, so information technology tools like computers can not be used. In other sectors like education, most of these developing countries have poor old education systems, so a student will not be aware of new information technologies