CHAPTER-VII
CHAPTER-VII
EMERGING THREATS OF INFORMATION TECHNOLOGY AND PRIVACY

7.1 An Overview

7.2 Privacy and Electronic Surveillance

7.3 Privacy and Internet

7.4 Privacy and Investigative Journalism

7.5 Recapitulation
7.1 An Overview

The classic definition of the privacy concept is that it consists of the 'right to be let alone' in terms of isolation from the scrutiny of others, the average individual living in a town or city enjoys vastly more personal privacy than did our ancestors living in small villages where every action was known to and a source of comment for neighbours. The right to privacy receives a measure of recognition in the European convention on Human Rights which provides that, "Everyone has the right to respect for his private and family life, his home and correspondence to an extent greater than with other basic human rights", the right to privacy must be subject to considerable qualification and, as epitomized in the ongoing debate concerning the allegedly intrusive nature of media activities, the right to privacy has to be balanced against other rights. One of the key distinctions drawn in discussions of the right to privacy is between an individual's private and public personae. In countries such as United States right to privacy ceases when an individual moves outside private property. In such circumstances, the act of watching an individual's movement tends to be considered under the title of 'surveillance'. In this chapter researcher is trying to discuss, Emerging threats of Information Technology and Privacy in respect of Privacy and Electronic Surveillance, Privacy and Internet, Privacy and Investigative Journalism.

In the past, 'surveillance' has been considered something which is primarily carried out by or on behalf of society as a whole (government). Although the act of placing an individual under surveillance may of itself modify individual's behaviour patterns, in general surveillance is a means to an end which may significantly affect other interests of the data subject. An obvious example might be the surveillance of an individual suspected of involvement in criminal/illegal activity. The act of surveillance may often lead to arrest, interrogation, trial and imprisonment. In 1971 Alan F. Westin in his seminal work information technology in a democracy identified three forms of surveillance; physical, psychological and data through digital satellite transfer.
Physical surveillance, involves act of watching or listening to the action of an individual. Such surveillance, even making use of technology, has tended to be an expensive undertaking capable of being applied to unlimited number of individuals. Example of psychological surveillance includes forms of interrogation or the use of personality tests as favoured by some employers. The end product of any form of surveillance is data or information. With both physical and psychological, surveillance, an active role is played by the watcher. Data surveillance involves different more passive approach. Every action of an individual reveals something about the person. This may occur directly, for example in filing out a form, or indirectly, as when goods or services are purchased.

Technology, like love, changes everything with the ability to digits any form of information, boundaries between the various forms of surveillance are disappearing with the application of information technology linking surveillance technique in to a near seamless web of surveillance. Developments in data processing suggest that a distinction between informational and physical privacy is becoming more and more filmsy. The reach of systems of physical surveillance has been increased enormously by the involvement of the computer to digitize and process the information received. Increased number of close circuit television monitor movement in the streets whilst countless thousands of cameras are operated by commercial operators to monitor our movement in the shops and offices and car parks. Surveillance through satellite cameras is increasing tremendously. The national remote sensing technologies of each space power countries are scanning the important data and digitalizing the information for various purposes such as crime prevention, scientific application, forecasting etc. Privacy therefore happens to be a serious concern in the age of video surveillance. Widespread usage of surveillance cameras raises the specter of an invasive ‘Big Brother’ society. In this regards, certain privacy laws have been introduced to guard an individuals privacy rights which will be discuss in the present chapter.
7.2 Privacy and Electronic Surveillance

- Electronic Surveillance

It is the monitoring of the behaviour, activities or other changing information usually of people and often in a surreptitious manner. It most usually refers to observation of individuals or groups by government organization, but disease surveillance, for example is monitoring the progress of a disease in a community. The word surveillance comes from the French word for “watching over”.

The word surveillance may be applied to observation from a distance by means of electronic equipment (such as CCTV cameras) or interception of electronically transmitted information (such as Internet traffic or phone calls). It may also refer to simple, relatively no or low technology methods such as human intelligence agents and postal interception.

Surveillance is very useful to government and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programmes such as Total information awareness programmes and advice, technologies such as high speed surveillance computer and Biometric software, and laws such as the Communications Assistance for law enforcement Act.

It is an often made statement that we live increasingly in surveillance society, primarily manifest in the public’s mind through the proliferation of CCTV cameras in our public and private spaces. Surveillance is both a crime prevention and detection measures, and has been greatly facilitated by developments in information and communication technologies. The nature of cyber crimes means surveillance is an important law enforcement tool in their detection and investigation. Surveillance may be carried out on a specified person’s, or persons’, communication activities such as emails or file transfers; or of a ‘virtual’ location in cyberspace where communications are exchanged, such as chat room or bulletin board. The surveillance may be put into operation at the edges of a network i.e. on a suspect’s terminal equipment.
as computer or mobile phone; or with in the network such as mail server, physically remote from the suspect.2

From a legal perspective, a clear distinction needs to be made between surveillance activities carried out by public law enforcement agencies in the course of an investigation and those carried out by private entities, such as employer and land owner. As a state based activity, the former is governed by strict rules of criminal procedure to protect individual rights, specifically a person's right to privacy.3

State authorized or Controlled surveillance may be carried out by personnel of the law enforcement agency itself, through the use of an informant, or require the involvement of a third party communication service provider to provide access to the forensic data, whether stared or in transmission and either created by the surveillance target or generated by the communication service itself. The obtaining of data from a CSP is examined separately in the following section, since data obtained from, or with the direct involvement of a CSP, may not always comprise a form of surveillance subject to regulatory control. Obtaining data from CSPs has also required a distinct legal framework and raises unique issues of concern.4

This section examines two categories of surveillance. Firstly, targeted surveillance, carried out by or under the authority of a Public LEA in the course of a specific investigation or operation, and subject to a distinct regulatory regime. Secondly, the more pervasive non targeted surveillance, here referred to as 'monitoring' and 'filtering', which is carried out by the state and private entities as a generic security measure, and is subject to a more opaque set of legal rules. Surveillance activities by public authorities in the course of a criminal investigation are monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; recording anything monitored, observed or listened to during course of surveillance; and surveillance by or with the assistance of a surveillance device.5
All these activities are clearly potentially applicable to investigative activities carried out in cyber crime environment, from the use of keystroke loggers, to “password” ‘sniffers’ and honey pots.

Directed surveillance is the most common form of surveillance activity used for detecting crime. It is defined by reference to four express characteristics. First, it is not intrusive, in the sense that it takes place in a public or quasi public space or location. Such as cyber café or where the surveillance occurs using a network resource remote from the physical location of the suspect, such as ISP – hosted web server. The second characteristics is that the surveillance be carried out in respect of a specific investigation or operation, rather than on a general basis, for example, the surveillance of person using a privately installed, unconcealed CCTV camera system in a shopping centre. The third characteristics of directed surveillance is that is likely to result in the obtaining of private information about a person; which includes any information relating to his private or family life. ‘Directed surveillance may only be carried out where it is necessary and proportionate response for achieving certain specified purposes, including in the interests of national security and the prevention and detection of serious crime.

- **Computer Surveillance**

The vast majority of compute surveillance involves the monitoring of data and traffic on the internet. In the united states for example under the Communication Assistance for law enforcement Act, all phone calls and broadband internet traffic (e-mail, web traffic, instant Messaging etc.) are required to be available for unimpeded real time monitoring by federal law enforcement agencies. There is far too much data on the internet for human investigators to manually search through all of it. So automated internet surveillance computers shift through the vast amount of intercepted internet traffic and identity and report to human investigators traffic considered interesting by using certain “trigger” words or phrases, visiting certain types of websites, or communicating via e-mail or chat with suspicious individual or groups.
• **Telephone and Mobile Telephones**

The official and unofficial tapping of telephone lines is widespread. In the United States for instance the communications Assistance for law Enforcement Act requires that all telephone and communications be available for real time wiretapping by federal law enforcement and intelligence agencies. In India wiretapping is generally regulated under the Indian Telegraph Act of 1885\(^{11}\), which gives the police authority to tape phones and intercept mail to aid an investigation.\(^{12}\)

There have been numerous wiretap scandals in India, resulting in 1996 decision by the Supreme Court that wiretaps are a “serious invasion on the individual’s privacy”.\(^{13}\) The court also set up guidelines for wiretapping by the government that defines who can tap phones and under what circumstances. Only the Union Home Secretary, or his counter part in the status, can issue an order for a wiretap. The court mandated the development of a high level committee to review the legality of each wiretap.\(^{14}\)

• **Surveillance Cameras**

Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device. IP network and/or watched by a security guard/Law enforcement officer. Cameras and recording equipment used to be relatively expensive and required human personnel to monitor camera footage. Now with cheaper production technique, it is simple and inexpensive enough to be used in home security systems and for everyday surveillance. Analysis of footage is made easier by automated software that organizes digital video footage in to a searchable data base and by automated video analysis software such as VIRAT or Human ID. The amount of Footage is drastically reduced by motion sensors which only record when motion is detected. In recent years, the use of video surveillance cameras to monitor public and private spaces throughout the world has grown to unprecedented levels. The leader in this trend is the United Kingdom, where it is estimated that between 150 and 300 million pounds per year is now spent on a surveillance industry involving an estimated 200,000 cameras monitoring
public places.\textsuperscript{15} Most town and cities are moving to CCTV surveillance of public areas, housing estates, car parks and public facilities. Some observers believe this phenomenon is dramatically changing the nature of cities. The technology has been described as the “Fifth Utility”\textsuperscript{16}. CCTV is being integrated into the urban environment in much the same way as the electricity supply and the telephone network in the first half of the century.

Their USC has come under greater criticism recently and recent research by the Scottish centre for criminology found that the cameras did not reduce crime, nor did they improve public perception of crime problems.\textsuperscript{17}

- **Aerial Surveillance**

  Aerial surveillance is the gathering of surveillance usually visual imagery or video from an airborne vehicle such as unmanned aerial vehicle, helicopter or spy plane.

  Digital imaging technology miniaturized computers and numerous other technological advances over the past decade have contributed to rapid advances in aerial surveillance hardware such as micro-aerial vehicles, forward looking infrared and resolution imagery capable of identifying objects at extremely long distances. For instance the MQ. 9 Reaper\textsuperscript{18}, A U.S. drone currently used for domestic operations by the department of Homeland security carries cameras that are capable of identifying an object the size of a milk carton from altitudes of 60,000 Feet, and has forward looking infrared devices that can detect the heat from a human body at distances of up to 60 kilometers.\textsuperscript{19}

  The United Kingdom as well is currently working on plans to build up a fleet of surveillance UAV ranging from micro aerial vehicles to full size drones, to be used by police forces throughout the U.K.\textsuperscript{20} In addition to their surveillance capabilities. Micro aerial vehicles are capable of carrying tasters for “crowd control” or weapons for killing enemy combatants.\textsuperscript{21}

- **Satellite Surveillance**

  Developments in satellite surveillance (also called “remote sensing”) are also occurring at a fast pace, and embrace features similar to those of more conventional visual surveillance since the end of cold war, companies such as
Earth Watch, Motorola and Boeing have invested billions of dollars to create satellites capable of mapping the most minute detail on the face of the earth.

A commercial satellite capable of recognizing objects the size of a student’s desk was launched from the U.S. in September 1999 and began releasing images in October 2000. The IKONOS is most powerful commercial imaging satellite ever built. Its parabolic lens can recognize objects as small as one meter anywhere on earth and the according to the company, viewers can see individual trees. Automobiles, road networks and houses. The satellite owned by Denver Company space imaging, will be the first of a new generation of high resolution satellites using technology formerly restricted to government security agencies.\textsuperscript{22}

The technology is already being used for a vast range of purposes from media reporting of war and natural disasters to detecting unlicensed building work and even illegal swimming pools. Meanwhile, governments are using satellites to regulate behaviour. Satellite tracking is being used to monitor convicted criminals on probation, parole, home detention, or work release, convicts carry a small tracking device that receives co-ordinate from global positioning satellites (“GPS”) and communicates them to a monitoring center.\textsuperscript{23}

- **Audio Bugging**

Advances in technology are also making it easier and cheaper to conduct covert audio surveillance. Bugs come in many shapes and sizes they range from micro engineered transmitters the size of an office staple, to devices no bigger than a cigarette packet than are capable of transmitting video and sound signals for miles. Many of the bugs are cleverly camouflaged. They are hidden in everything from umbrella stands to light shades. Sometimes, the infiltrator will hide them in a business or sports trophy where they will stay indefinitely. The latest bugs remain active with their own power supply for around ten years.

Laws restricting the use of covert audio devices vary widely across the world. Many countries have provisions in their general wiretap laws that also cover the use of bugs. The European Court of Human Rights has rules several
times that all signatories of the convention must enact laws governing their use.\textsuperscript{24}

- **Location Tracking**

  The rapid development of wireless communications systems has brought a new privacy issue to the forefront: the collection and use of location data. Some generation of location information is inherent to the functioning of a wireless network; for instance, a wireless telephone call can not be completed unless the network is able to detect the cell tower that is nearest to the handset. While cell tower location tends to be imprecise and incapable of pinpointing the location of a user, new initiatives are driving the development of technologies that can determine an individual's location much more precisely.\textsuperscript{25}

  Recognizing the privacy implications of the automatic location identification (ALI) requirements, Congress enacted location privacy provisions in the wireless communications and public safety Act of 1999.\textsuperscript{26} The Act requires "express prior authorization" by a consumer to approve "the use or disclosure of or access to" his or her call location information" for purposes other than emergency services.

### 7.3 Privacy and Internet

Human beings have experienced over the last few centuries, two major revolutions: the industrial revolution and the electronic revolution. The former transformed our society from being agriculture based to industrial based, whereas the latter transformed our society from being mechanical based to electronic based. Turban beautifully sums up the scenario as: "As we entered the 21\textsuperscript{st} century, we are seeing the beginning of a new revolution, namely the network revolution. It interconnects different parts of the world, enabling the seamless flow of information the internet is the engine of this revolution and electronic commerce its fuel". With the introduction of the world wide web-electronic commerce has revolutionized traditional commerce and boosted sales and exchanges of merchandise and information.

Computer nowadays make the collection, maintenance and manipulation of personal data more possible, faster, less expensive and more effective than
manual methods. A serious concern for individual privacy, therefore, is growing right alongside the growth of e-commerce. Privacy is the ability of individuals to control information about themselves what and how much is collected, how it may be used, and so on.\textsuperscript{27}

Fifty years ago, George Orwell, the English writer, whose fears for the loss of individual liberty dominated his novels, imagined a totalitarian state where advanced technologies would be used to monitor the people in all their endeavors. ‘Big Brother’ would be watching us and privacy would be a thing of the past; Orwell’s fears stand some what true in this era of information and communication revolution (ICR).

The new technologies have enhanced the possibilities of invasion in to the privacy of individuals and provided new tools in the hands of eavesdroppers. Individual privacy is at a greater stake than ever before. Computers and Internet can be used to a mass huge amount of data regarding people, profit it in various ways, commodity it and deal with it in a manner which could violate individual’s privacy.\textsuperscript{28}

Computer and Internet have created an environment in which there is inexpensive and ready access to an ever growing pool of personal information about identifiable individuals any where in the cyber world. “Privacy in the technology driven world is a difficult proposition. Technology has become a kind of double edged sword, on one hand it equips the person to safeguard his privacy and on the other it helps in blowing the privacy cover, one may had.\textsuperscript{29}

With information and communication revolution pacing fast to broaden its horizon, the Internet has become the fastest growing means of communication through e-mails, chats, browsing, etc. There is an increasing reliance on computers concerning all facets of life. For example, we trade and communicate with the help of computers and the Internet, obtain many services – medical advice, ticket reservation, ordering food etc. on the internet. All this has changed the structure of the society in a way that the computer today occupies a very important place in our lives. This leads to cyber paradox – on the one hand, the computer and the Internet have accorded extreme privacy and
on the other hand the same tools of technology allow the gagging of privacy. Today, information superhighway is not really the safest place to be.\textsuperscript{30}

The internet is a rich source of personal information about online potential consumers. Some of the website owners follow the consumer’s online activities and gather information about personal liking and disliking. The data so collected to target marjet products and services but on the basis of such data they may also sell advertising space on their websites. The personal information data may be recorded by government department, various service providers and other organizations like insurance company, banks, hospitals, schools, credit card co. telephone service provider etc. This personal information may be misused if fallen in wrong hand. Mr. Bill Gates in his book “The Road Ahead” has expressed his concerns relating to privacy- “Loss of privacy is another major worry where the network is concerned... The potential problem is not the mere existence of information. It is the abuse that makes me worry”.\textsuperscript{31}

In 2003, a 24 years old engineer from Delhi earned the dubious distinction of being the first person in India to be convicted for a cyber crime. The case was registered following a complaint from Sony India Limited against the accused. It was alleged that this young man, who was employed at a call centre of the electronics company, managed to chat with a woman in the USA and obtain her credit card details on the pretext of updating her bills. He used the same credit card number and brought himself a colour television and a cordless phone through Sony Sambandh.Com, a Sony website for the NRIs the cost of both item was $578. Barbara Campa, the holder of that credit card number complained to the company that the transaction was ‘unauthorized’ after purchasing the items; the accused moved these to a new address in Gurgaon. However, a photograph taken by Sony officials when making delivery undid his plan- CBI officials soon traced the transaction to the call centre through IP address. After a seven month trail, the accused finally cracked.\textsuperscript{32}
Computer crimes are different from the usual crimes, vis-à-vis investigation. There are no usual evidentiary clues, no documentary evidences. Even the Computer misused may have only erased data which may be beyond the comprehension of a usual investigator or even of an expert. Computer crimes are difficult to investigate because computer crimes are hi-tech crimes. The information technology is changing very fast.

The cell have private computer specialists, honest and reliable who can provide technical know-how for the purpose. A computer crime may be committed in one country while the resultant fallant may be in another country. Besides, jurisdictional problems arise. The computer satellite computer link can be anywhere. A debit or credit card can do the trick anywhere, sale terminals, ATMs, EFT etc are good enough for the purpose. The criminal has just to drum a keyboard and drums of money are taken away, without personal exposure, no written documents, no signature, no finger prints, no voice. The criminal is truly faceless. The commission of computer crimes is done with element. It may take days, weeks, even relating to the time lightening speed without leaving any trace relating to the time element. It may take days, weeks, even month and years before the crime are discovered.33

The cyber world and its related crimes have no territorial barriers, and this makes everything complex because evidence is very hard to come by. As global companies and governments join e-market places and business becomes boarder less, their vulnerability multiplies. Privacy in these e-markets would be a major area of concern in the coming days, with greater degree of damages what is of far greater serious concern is that cyber worms can turn everything upside down alone with a laptop at his weapon sitting in a basement or in a bathroom connecting it with a mobile phone. And damages can take place in a matter of few seconds along with these damages there are harassment in several forms to an individual or a group of people online, breaking all barriers of privacy. With the privacy issue at centre stage, cookies, spamming, web tracking; and hacking and Spyware are important areas of discussion of this
present area of thesis by which insecurity from the technological front arise and surveillance on Internet is being done.\(^34\)

- **Cookies**

  Web sites are increasing day by day and most of the websites dealing with e-business are getting technologically smarter. They know more about a visitor each time he visit the site for example, when one visits a web site, the computer on the other hand records the time of the visit, whether or not he has visited them before, when he last visited, what he was trying to find out in that particular website, his e-mail address and other customizable information. There is a race to acquire more and more information about the perspective customers and find out their consumption preference and buying behaviour. All this data about a person may be collected without knowing about it. Most websites achieve this stunning feat with cookies.

  A cookie is information that a website puts on one’s hard disk so that it can remember something about him at a later time. Typically a cookie records your preferences when using a particular site. Using the web’s Hypertext Transfer Protocol (HTTP), each request for a webpage is independent of all other requests. For this reason, the web page server has no memory of what pages it has sent to a user previously or anything about your previous visits. A cookie is a mechanism that allows the server to store its own information about a user on the user’s own computer. The user can view the cookies that have been stored on his hard disk. The location of the cookies depends on the browser. Internet explorer stores each cookie as a separate file under a windows subdirectory. Netscape stores all cookies in single cookies. Txt file opera stores them in a single cookies file.\(^35\)

  Cookies are commonly used to rotate the banner add that a site sends so that it doesn’t keep sending the same add as it sends the user a succession of requested page. They can also be used to customize pages for the user based on his browser type or other information that he may have provided the website. In general cookies help websites to serve users better. However, the existence of cookies and their use is generally not concealed from users, who can also
disallow access to cookie information. Nevertheless, to the extent that a
website stores information about you in a cookie that you don’t know about,
the cookies mechanism could be considered a form of Spyware.36 ‘Shopping
Carts’ are good examples of cookies in action. When a user browses a series of
WebPages for items to buy and finds something he is looking for, he adds it to
his shopping cart by clicking a button on the page. And later, he can view all
these items together. The most important area of concern is that even though a
person communicates through an ‘anonymous’ connection, the website always
knows exactly what is in one’s personal shopping cart. It does not matter
whether the person clicked away to some where else and comes back, or even
if the person has completely shutdown his computer and returns days later. The
website still knows who that person is and what he was shopping for. This is
because; when a person visits the same website again his browser sends the
cookie to the web server. The server can use this information to present him
with customized WebPages. In that case, instead of seeing just a generic
welcome page, he might see a welcome page with his name.

“Once a site has assigned your computer a unique identification code it
can collect the entire click stream data created by visits using your computer,
and associated those data with your identification code. Thus a website can
create a dossier of information that is associated with your computer, and can
use this information to personalize its interaction with you.”37

Cookies can be used to track people to gain statistics as they go through
the website. Because every time we visit a website, we have a footprint of
personal information about ourselves like our preferences, websites we visit,
our financial matter etc.

This rather simple capability has profound implications for the privacy
of website visitors. While cookies do have uses for both the user and web
providers and are even helpful, they can be misused. Beneficial to the user
when dealing with a company that has a good privacy policy in place, it is of
questionable value when left open and available to the world at large. The real
problem is with aggregation of data from multiple sources resulting in a user
profile. Collected personal information is now being treated as a commodity belonging to the collectors. Many users do not go beyond the knowledge that cookies exist and websites take advantage of the user’s inexperience and collect, catalogue and commodity information totally unwarranted.

The information technology Act, 2000 does not deal with cookies but section 43(b)\textsuperscript{38} says that if any person without permission of the owner or any other person who is in-charge of a computer, computer network, downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Cookies are meant to extract data from a computer and if planted without permission could lead to liability under section 43 (b).

Further Section 43(c)\textsuperscript{39} says that if a person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network, he shall be liable.......computer contaminant has been defined as any set of computer instructions that are designed to modify, destroy, record, transmit data or programme residing with in a computer, computer system or computer network\textsuperscript{40}. Cookies would come under the definition of computer contaminant as they are designed to record and transmit data residing within a computer. If a website sends cookies to a user’s machine while he is visiting that website without his permission, the website could be held liable under Section 43 of the Information Technology Act.

- **Web Bugs**

  A web bug, also known as web beacon, is a file object usually a graphic image such as a transparent GIF\textsuperscript{41} that is placed on a webpage or in an e-mail message to monitor user behaviour, functioning as a kind of spyware.\textsuperscript{42} The word “bug” here is being used to denote a small, eavesdropping device and is not a euphemism for a programming error. Unlike a cookie, which can be
accepted or declined by a browser user, a web bug arrives as just another GIF on the webpage. A web bug is typically invisible to the user because it is transparent and takes up only tiny amount of space.

It can usually only be detected if the user looks at the source version of the page to find on IMG tag that leads from a different web server than the rest of the page. A web bug can send several pieces of information to the server computer, and those includes, the IP address of the computer that fetched the web bug, the URL of the page that the web bug is located on, the URL of the web bug image which contains the information to be communicated between the web page visited and the site collecting the data, the time the web bug was viewed, the type of browser that fetched the web bug, image and the identification code contained in any cookies that was placed by the server. Web bug can be used to provide an independent accounting of how many people have visited a particular website. In addition, advertising networks can use web bugs to collect information on what sites a person is visiting to create a personal profile which is stared in a data base server belonging to the advertising network and identified by the browser cookie of the network. A web bug is more powerful than a cookie because of its ability to transmit information to a server other than the one that holds the web page the visitor is viewing.

Technological innovation are very fast, and now web bugs can be found in various other applications like e-mail, documents produced by word processing, spread sheet, presentation and other software applications. “E-mail messages that display graphics and styled text are constructed out of the same HTML code that constitutes web pages, and are equally capable of harboring web bugs. Such as bug might consist of an instruction to fetch an invisible graphic from the e-mail sender’s server, and while doing so transmit information back to the server.” For example, when an e-mail user open his e-mail in box and read the message the web bug can “Call home” and it can report back the time and date the user opened it. The sender thereby comes to
know this information. Although proponents of Internet privacy object to the use of web bugs in general, they also concede that web bugs can be put to positive use, for example to track copy right violation on the web.

No body can enter some one’s house without his permission. Even if law enforcement agencies need to search a premise, they have to go through a legal process and require search warrant. But through web bugs a computer can be subjected to search without following any legal procedure. This is gross violation of privacy especially at a time when a computer has become the storehouse of a person’s most valuable information. If a web bug is planted in a computer without the permission of the owner of the computer, it could lead to liability under section 43(b) and (c) of the Information Technology Act.45

- **Hacking**

Hacking is ‘unauthorized access’ to a computer and refers to access to the whole or any part of a computer system without permission. Hackers world wide attempt to hack into remote computer systems for multiple purposes like eavesdropping, data theft, fraud, destruction of data, causing damage to computer systems, or for more pleasure and personal satisfaction.46

According to the Merriam-Webster’s collegiate dictionary hacker has two definitions. The first one defines hacker as ‘An expert at programming and solving problems with a computer’ and the second ‘A person who illegally gain access to and sometimes tampers with information in a computer system.’ A hacker is now being used as a generic term for referring to people who get into other’s computers systems and networks.47

The meaning of the term hacking has evolved over time but is still applied some what variably to a complex mix of legal and illegal activities ranging from legitimate creative programming techniques to illicit lock picking and manipulation of world wide phone/computer systems.48

At the basic level, hackers are considered to be learners and explorers who want to help rather than cause damage, and who often have very high standards. A Hacker may not indulge in vandalizing or maliciously destroying data, or in stealing data of any kind. But the term Hacking has acquired dual
meaning today and a hacker may variably mean a cyber burglar or vandal, and
individual or group who believes in causing malicious harm to a network or
computer, or to steal information like passwords, credit card numbers, names
and address, financial information, even the account information for the ISP,
and in short anything stored on a computer.

One example of Hacking software is a Trojan horse program, in which
malicious or harmful code is contained inside apparently harmless
programming or data in such a way that it can get control and do this chosen
form of damage, such as running the file allocation table on a hard disk.49

Trojan horse is snooping software, which may come as an e-mail borne
virus. The Trojan horse may even be able to record each and every key stroke
one makes, save the information to a Hidden file and then when one goes
online, upload the file to the hacker’s computer. This means that even if you do
not keep personal information or passwords on your computer the hacker can
still obtain them from the keystroke log he uploaded50. One of the most recent
uses of Trojan horse is to cause DDos (Distributive Denial of Service) attacks.
In a DDos attack, the client commands all of the ‘servers’ located on individual
PCs to attack a single website. Thousand of individual PCs can be commanded
to access a website like e-Bay or Yahoo at the same time, clogging the site’s
band width and causing on interruption of service. The most worrisome point is
the ease by which these attacks have been carried on. The software to do this
damage is simple to use and readily available at underground hackers sites
through out the Internet. A tiny program can be downloaded from these sites
and then, with the push of a button the PCs are alerted to go into action all over
the world, sending a simple request for access to a site, again and again scores
and hundreds of times a second.

There are several cases registered or unregistered related to hacking in
India for examples are: Zee TV. com. job.com etc., and notorious group of
Pakistan hackers called G-force during 2001 hacked many websites of Indian
organizations, for example, Indian science congress Asian Age Newspaper,
National Research Centre, Agricultural University of Maharashtra, IIM
In 2002, the website of Assam tourism Department was hacked by unknown hackers, perhaps the most shocking instance of hacking in India’s, when a 15 years old American boy, with a strange name t3k-9 hacked in to the Mumbai based Bhaba Atomic Research Centre (BARC) Computer network, soon after the Pokhran nuclear tests, during May 1998. He passed on the information to his friend named ‘Iron Logik’, an 18 year old immigrant from Serbia, and placed the list of 800 BARC login names and passwords to a hacker channel. Again a group of hackers who call themselves ‘Armagedon’ gained access to an Indian Bio Medical Research Facility during 1998 and stolen the test results and internal memos on the possible effects of nuclear tests on the country’s environment and civilian population. So from individuals to e-commerce websites to the websites of governmental organizations and their databases may be targets of hackers.

Section 66 of the Information Technology Act deals with hacking with computer system, states:

1. Whoever with intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alerts any information residing in a computer resources or diminishes its value or utility or affects it injuriously by any means, commits hacking.

2. Whoever commits hacking shall be punished with imprisonment up to three years or with fine which may extend up to two lakh rupees, or with both.

Computer hacking has come in to existence due to a need and intellectual activity. Slowly the criminal component in hacking activities started rising and with a result, now the society viewing hackers as criminals. Criminal hackers can pose grave threat to the organization as well as individual privacy.
• Spamming

Spam is unsolicited e-mail, through which a message is delivered, over the internet, to someone who would not otherwise choose to receive it. Most of the spam is commercial advertising. It also refers to sending an e-mail message to hundreds and thousands of Internet users.\(^{54}\) It's roughly equivalent to unsolicited telephone marketing calls except that the user pays for part of the message since every one shares the cost of maintaining the Internet.\(^{55}\)

It is an attempt to deliver a message, over the Internet, to someone who would not otherwise choose to receive it. Almost all spam is commercial advertising. From the sender's point of view, it's a form of bulk mail, often to a list obtained from a spambot or to a list obtained by companies that specialize in creating e-mail distribution lists. Potential target lists are created by scanning use net postings, lifting, internet mailing lists, or searching the web for addresses. The commercial web sites also gather information with automated searches to retrieve e-mail addresses. They use cookies and get help through data mining. Suppose a person wants to buy a washing machine, so he visits a websites selling washing machine suddenly, a few days later when he browses the web, he gets e-mail containing advertisement for washing machine. So there is somebody sitting on the other side collecting information about a person without him knowing that. The low cost of e-mail spamming offered for sale with millions of e-mail address, coupled with the fact that the sender does not pay extra to send e-mail, has resulted in the current explosive growth of Junk e-mail. In many instances, the message may be large and data may be meaningless. The effort is to consume additional system and network resources, thereby abusing multiple accounts at the target site and increasing the denial of service impact. It annoys, it invades privacy and creates online traffic jams.

Some States in the USA like Nevada, California, Virginia, Colorado, Maryland, Rhode Island and Washington have passed anti-spamming legislations, i.e. legislations targeting only spamming. There are several other federal legislations, related to spamming and unsolicited commercial e-mails,

The issue of spamming has not been directly deal with in any Indian statute. Spam is an unsolicited message requiring one’s time and effort to get rid off. A regular supply of such spam messages would naturally result in considerable annoyance. So, the law of nuisance under tort law can be used for bringing the spammer to books. Continuous spam could also cause disruption, damage or denial of service to a computer. In case any person is receiving a voluminous, regular supply of spam messages, recourse could be had to sec 43(d), (e) and (f) of the Information Technology Act which make damage, disruption to any computer or data or programme illegal.57

- **Spyware**

Spyware is another threat to privacy of an Internet user. “Some software developers have included code (Trojans, Backdoor Santas, Ad ware or Drive by Downloads, etc.) with in their applications that cause the user’s computer to transmit information back to the software developer via Internet.”58 Spyware can be used for generating annoying pop-up advertisement, collecting passwords and credit card numbers etc. Spyware is one type of malicious software that collects information from a computing system without the consent of the user. Spyware can capture keystrokes, screenshots, authentication credentials, personal e-mail addresses web from data, internet usage, and other personal information. This data is often delivered to online attackers who sell it to others or use it themselves for marketing or spam or to execute financial crimes or identity theft.

The people who use Spyware include

- Online attacker
- Marketing organizations
• Organized crime
• Trusted insiders
• Online Attacker

Online attacker’s primary interest in Spyware is using it to steal personal information for financial crimes such as carding (illicit trafficking in stolen credit card) and credit card information and identify theft, or to sell that information to someone else who then executes more traditional financial crimes.

• Marketing Organizations

Marketing organizations are interested in personal information such as e-mail addresses, online shopping and browsing habits, key words in search queries, and other personal and trend-related information that can be used to execute campaigns like spam, spin (unsolicited messages received via instant messaging systems), browser pop-ups, home page hijacking, and more.59

• Spying by a Trusted insider

Trusted insiders include who have physical access to computer systems for legitimate purposes. Some examples are employees, contractors, temporary workers, and cleaning crews. A trusted insider might be, for example, an employee who uses Spyware to collect corporate information that can be sold in the underground economy, used for blackmail, or used to gain access to more valuable information at some later time.

Another example of the trusted insider group includes family members or close relations such as spouses or significant others trying to catch inappropriate behaviors or infidelity.60

Date Gathered by Spyware can monitor nearly any activity or data related to your computing environment. This is not limited to files on your hard drives but can also include temporary data such as screen shots, keystrokes, and data packets on connected networks.

Spyware can cause people to lost trust in the reliability of online business transactions. Similar to the problem of counterfeit currency in the physical world, Spyware undermines confidence in online economic activity.61
7.4 Privacy and investigative Journalism

The freedom of speech and expression enshrined in Article 19(1) (a) of the Indian Constitution is considered as the soul of any democracy. It is a natural right which every citizen acquires on his birth. It has been opined that every citizen has the right to freedom of opinion and expression; the right includes the freedom to hold opinion without interference and seek, receive and impart information on any ideas any media and regardless or frontiers.

Freedom of media & press is not a virtue in itself. It is not specifically worded under the Indian Constitution under Article 19(1) (a) but such freedom is embedded under the constitution through judicial pronouncement and through experience of other countries.\(^\text{62}\)

The philosophy behind such freedom of press is to advocate public interest and to provide a platform through which free and fair public opinions can be spread with the burgeoning and exponential growth of media, the concept of freedom of press was considered to be a perennial right. Further dimensions to the freedom of expression is added by the existence of mass society in which communication among citizens can take place only through the use of media like the press and broadcasting not directly.\(^\text{63}\) A free press is the verb basis of democracy. But there had been persistent opposition to freedom of press and to all democratic movements from the government all over the world. Freedom of press, as it is today is the result of few centuries hard won fight in the name of the people.\(^\text{64}\)

The freedom of press is basically the freedom of individuals to express themselves through the medium of press this freedom of press is fundamental to the life of an individual in the democratic polity. The concept of free press was explained by ‘William Block Stone’ long ago in 1769 in the following words;

“The liberty of press is indeed essential to the nature of a free state; but this consists in laying no previous restraints upon publications and not in freedom from censure from criminal matter when published. Every free man has an undoubted right to lay what sentiments be pleases before the public; to
forbid this, is to destroy the freedom of press; but if he publishes what is improper, mischievous, or illegal he must take consequences for his own temerity. To subject the press to the restrictive power of licensor-is to subject all freedom of sentiments to the prejudice of one man, and make him the arbitrary and infallible judge of all controverter points in learning, religion and government. But to publish — any dangerous or offensive writing, which, when published, shall, on a fair and impartial trial, be adjudged of a pernicious tendency, is necessary for the preservation of peace and good order of Government and religion, the solid foundation of liberty”.  

The view of Prof. AV Dicey also sounded similar to that of black stone where he says: “The freedom of press means the right of a person to publish what he pleases in books or newspapers” but the laws of England do not recognize any special privilege attached to the press. The first Royal Commission on Press (1947-48) however, chooses not to discuss the meaning and significance of the press. The another Royal commission on the press emphasized the freedom of press as, “that degree of freedom from restraint which is essential to enable proprietors, editors and journalists to advance the public interest by publishing the facts and opinions without which a democratic electorate can not make responsible judgment”.

The media in India theoretically enjoys the same freedom that is guaranteed to every citizen. As an institution it has no constitutional or legal privilege. The right flows from the right to freedom of expression that is guaranteed under Article 19 of the Constitution. Such a right is not absolute and is subject to reasonable restrictions, Article 19(2) laid down the restrictions on this right to freedom of speech and expression and the freedom which is guaranteed to the press is no exception to this.

Contrary to the constitutional mandate in Indian Express Newspapers v. Union of India Court is of the view that the Freedom in our context is absolute, so long as, it does not violate reasonable restrictions highlighted in clause (2) of Article 19 of the constitution. State or its functionaries can resort to these reasonable restrictions given below in adversely affecting or abridging or
curtailing or transgressing the freedom of press or individual in the matters relating to:

(a) Sovereignty and integrity of India
(b) Security of state
(c) Friendly relations with foreign states
(d) Public order
(e) Decency or morality
(f) In relation to contempt of court
(g) Defamation or incitement to an offence.

The quality of freedom has been fully qualified by the concept of privacy or the right to privacy. The term right to privacy has not been specifically and categorically defined in the constitution or under any other law.

In common parlance the term right to privacy means; right to live in one’s own way. It means one has right to do what one likes to do with one’s own life of one has right to do what one likes to do in his own style without interference of any kind by any one and without impairing decency and dignity of others or intruding into the privacy of others in any manner whatsoever.

The term privacy may be equally interpreted as “right to seclusion” or “right to be let alone”. The right to privacy encircles within the concept of dignity and decency also. This right has element of secrecy or confidentiality. The right to privacy implies the right not merely to prevent incorrect portrayal of private life but the right to prevent its being depicted at all. The right has multi pronged dimensions. In personal intimacies, it extends to home, family marriage motherhood procreation and even child bearing, consistent with the dignity and decency. It further includes with in it, right to use contraceptives, use or abuse of sex and personal habits even obnoxious one. Right is also extendable in professional relations and personal communities. The right extends to the publication of private affairs like details of illness or disease of a person etc.\textsuperscript{72}

In the present day society, it is inevitable to strike a proper balance between right to freedom of press and right to privacy with the unprecedented growth of
media and technology. Presently media has taken a paradigm step, earlier when media was not such potent or active their was very less concerns about the right to privacy and intrusion in one’s personal life. Advances in Computer technology and telecommunication have dramatically increased the amount of information that can be stored, retrieved, accessed and collated almost instaneously within this context; it is with caution that one approaches the issue of Privacy, for any such discussion would actually involve further restricting the media’s freedom. But as a collective, the media in India is an extremely powerful institution that often tramples upon individual rights, especially of those who are not in a position to assert them. In such situation ‘privacy’ or ‘the right to be let alone’ is a necessary requirement to insulate these individuals from public attention.

The focus in this chapter is not on public figures who would want to keep their private lives out of the public eye. This is not to belittle their concerns. The release and circulation of sexually explicit tapes of a political leader does raise some grave questions on ethics and privacy, even if one were to accept the fact that public figure in view of their position will be scrutinized severely by the media. Media releases of photographs of actor Kareena Kapoor found kissing her boy friend prompted the Supreme Court to ask whether such pictures served any ‘public interest’ But such persons, by virtue of their positions, enjoy privilege and power in the Indian context and have the where with all to take recourse to remedies available under the law. Such privilege’s are however not available to the vast majority of persons who are then exposed to great risks by such media exposure. Few incidents of privacy are as follows:

In a public hearing on children’s rights in Chennai, child survivors of rape were photographed by some media persons despite repeated requests by the organizer not to do so. One of them responded that if the organizers did not want journalists to take photographs, they should not have invited the media in the first place.
The hearing was public, in as much as the survivors narrated their experiences with the judicial system to a select group working on children’s rights as well as to members of the Jury. The focus of the hearing was to raise awareness about the problems faced by survivors in child sexual abuse trials; it was not to expose children to media attention. The concerned media persons, however, were clearly not willing to distinguish between the public interest that was involved in discussing sexual abuse of children and the latter’s right to privacy.

In another incident, the Chennai police conducted a series of raids on some residences. The police claimed that brothels were being run in the premises. Photographs of women alleged to have been found during the raid were released to the media. Sections of the media published the pictures of women along with the phone numbers and addresses of the premises. No questions were raised about the modus operandi of the raid or about the lives of the women. As far as the media was concerned, the women alleged to be sex workers had to be exposed with a crusading zeal. Needless to say, not a single male was photographed by the media.

Third incident relates to the media coverage of two children who were found to be HIV positive in Kerala. The children were removed from school by the authorities after their status was revealed, and the media did serve valuable public interest by raising a furore over the matter. But in the process the children’s pictures were once again published in some newspapers and television channels, their by making their identities known to everyone.\(^{75}\)

Any discussion on privacy would necessarily involve addressing the public private divide. Issues relating to violence against women and children have for too long been considered as matters to be kept with in the private sphere and hence hidden from public gaze. Arguments concerning honour and family values are often used to prevent survivors from seeking Justice in the face of violation. Bringing such issues out of the private sphere has therefore been a great challenge. However, at the same time, issues involve individuals, and such individuals need to be protected from the prying eyes of the public.
To such individuals privacy is of utmost importance, since public exposure can have serious repercussions, some of which may be fatal.

In the first and third incidents given above, public interest was definitely involved. The media has a powerful role to play in focusing on such issues. However, at the same time, it has a responsibility to perform a balancing act by not revealing the identity of the persons concerned. As far as the second example is concerned, it is my view that no public interest was served. On the contrary, release of such news and pictures harmed the women concerned, apart from reinforcing patriarchal norms.

'Privacy' is a recent development in the area of law, but it has been recognized as a human right. The first Judgment of the Supreme Court on the subject related to the intrusion of the privacy by surveillance. The court held that domiciliary visits by the police without the authority of law is a violation of privacy that flowed from Article 19(1)(d) of the Constitution relating to freedom of movement and Article 21 relating to the right to life.

However it was only in R. Rajgopal v. state of Tamil Nadu, that the Court addressed the right to privacy of the individual referred to in a publication. The Tamil weekly Nakeeran Serialized an autobiography of a death row convict Auto ‘Shanker’. In his autobiography Shanker narrated his rise and how it would not have been possible without the connivance of many persons in high places, and these were mentioned by name. Shanker was in prison and the dispatches, according to the editor, were sent from prison. The prison authorities stopped the dispatches, prompting the editor, Rajagopal, to challenge their order in Court. Shanker in the meanwhile, refused to acknowledge the serial as his own, presumably under pressure form the prison authorities.

While the case before the apex court was on the right to free expression, the court examined the right of privacy in detail and laid down the following directions:

(a) The right to privacy is implicit in the right to life and liberty guaranteed under Article 21 and is a ‘right to be left alone; A citizen has a right to
safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education, among other matters without his consent whether truthful or otherwise and whether laudatory or critical. If one does so, one would be violating the right to privacy of the person concerned and would be liable in an action for damages. The position may, however, be different if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.

(b) The rule becomes an exception if the publication is based upon public records including court records. This is because once a matter becomes a matter of public record, the right of privacy so longer subsists and it becomes a legitimate subject for comment by the media. However in the interests of decency Article 19(2), an exception is carved out of this rule, viz, a female who is a victim of sexual assault, Kidnapping, abduction or a like offence should not further be subjected to the indignity of her name for the incident being publicized in the media.

(c) In the case of public officials, right of privacy is not available with respect to their acts and conduct relevant to the discharge of their public duties even when the publication is based on facts and statements that are not true, unless the official establishes that the publication was made with reckless disregard of truth. In such a case it would be enough for the media to establish that they acted after a reasonable verification of facts and it is not necessary for the media to prove that what was published was true unless the publication is proved to be false and actuated by malice or personal animosity.

(d) Government, local authority and other organs and institutions exercising governmental power can not maintain a suit for damages for defamation.

(e) The Official Secrets Act or other enactments having the force of law binds the media.

(f) No law empowers the state or its officials to prohibit or impose a prior restraint upon the media.
The Court observed that the principles are only broad, neither exhaustive nor all comprehending—indeed no such enunciation is possible or advisable.\textsuperscript{80} In \textit{Sharda v. Dharmapal},\textsuperscript{81} the Supreme Court held in the context of a case involving a matrimonial dispute that “to allow private communications to be publicly disclosed abrogates the very fiber of an individual’s right to privacy ...” and that such communications may be made public only” if the benefit to society out weigh the costs of keeping the information private.

In \textit{R. Sokanya v. R. Sridhar & others},\textsuperscript{82} the Court held that the right to privacy created by the statute has to be preserved. The very inception of the provision, Section 22 in the Hindu Marriage Act makes it clear that matters pertaining to matrimonial affairs are intended to be conducted ‘in camera’ and not intended to be divulged to others, except publication of the Judgment with the leave of the court. Right of privacy in matrimonial matters between the parties in litigation under marriage Acts is personal to the litigating parties. Thus it is manifestly clear that the legislature has intended to guard the right of privacy in relation to matrimonial matters and it is settled legal position that real meaning and effect should be given to the world employed in the statute. In this case trial court dismissed the said matter, on the ground that the respondent has not contravened the provision of Section 22 of the Hindu marriage Act and that they are not liable for any punishment under the provision of the said Act and if they contravene the said provision action has to be taken before the appropriate forum.

Modern investigation Journalism is a discipline rigorous and demanding. Modern Journalism, despite its many aberrations, is considered the most effective monitor and up holder of democratic values. And the powerful instrument to fulfill this obligation is investigative reporting. Democracy involves accountability of elected representatives and civil servants. There are many mechanisms for checks and balances, but these can be abused, circumvented, ignored or made ineffective. Investigative reporting steps in to his vacuum to scrutinize and expose the wrong doing of those in authority which hurt public interest and make them accountable to the people.
Investigative Journalism is a type of reporting in which reporters deeply investigates a topic of interest, often involving crime, political corruption, or some other scandal.

DE BURGH states that, “An investigation journalist is a man or woman whose profession it is to discover the truth and to identify lapses from it in whatever media may be available. The act of doing this generally is called investigative journalism and is distinct from apparently similar work done by police, lawyers, auditors and regulatory bodies in that it is not limited as to target not legally founded and closely connected to publicity”.

An investigative journalism may spend a considerable period researching and preparing a report, sometimes months or years, where as typical daily or weekly news reporter writes items concerning immediately available news. Most investigative journalism is done by news papers, wire services and freelance journalists.

As journalism is entering a new phase of revolution the emerging challenges are adding a fresh approach. Sting operations are certainly getting popular and demanding in India. Most discussions about ethics in investigative journalism have focused on the methodology what methods are valid to reveal wrong doing? Is deception legitimate when the aim is to tell the truth? Can television reporters use hidden cameras to get the truth? Can journalists use false identities to gain access to information? In this chapter, an attempt has been made to find out the answer of these questions.

Sting operation is a complicated confidence game planned and executed with great care especially on operation implemented by under cover agents to apprehend criminals.

In law enforcement sting operation is an operation designed to catch a person committing a crime, by means of deception. A typical sting will have a law enforcement officer or cooperative member of the public play a role as criminal partner or potential victim and go along with suspect’s actions to gather evidence of the suspect’s wrong doing. For examples:

- Purchasing illegal drugs to catch a supplier.
- Deploying a bait bar to catch an auto thief.
- Posing as a client to catch a prostitute or pimp/escort agency.
- Posing as a prostitute to catch a client.
- Posing as some one who is seeking child pornography to catch a suppler.
- Posing as a supplier of child pornography to lure a child molester.
- Posing as a child in a chat room to lure a child molester.
- Police arranging some one under the legal drinking age to ask an adult to buy alcoholic beverage for him or her.\[^{86}\]

**Different Types of String operation:**

- **Honey trap**

  A honey trap is a form of sting operation, in which wrong doers are lured into revealing themselves to a policing organization, where a sting operation targets a known or suspected individual and attempts to trap them committing a specific case of crime; a honey trap establishes a general lure to attack unknown criminals. So for example, the police might fit a bait car with hidden cameras and leave it in an area known for its problems with car crime as a honey trap. The expectation being that the far will be eventually be stolen, recording the evidence in the process.\[^{87}\]

- **Espionage Usage**

  In spy terminology honey pot (Espionage) has been used by soviet, Cuban and Eastern European intelligence services defining a women entrapping businessman and officials from the west in sexual liaisons to retrieve intelligence and to achieve subservience. The most well known case in this regard happened in the 1980s when the U.S. Marine corps sergeant Clayton J. Lonetree was entrapped by a female soviet officer with revealing photographs. Consequently the term is used in detective novels and espionage novels to describe a trap using some form of sexual enticement. On the Internet, the Honey net project attempts to attract and watch hackers breaking into a number of network systems. In particular it monitors changes in routine and automated hacker activity, such as port scanning.\[^{88}\]
- **Badger Game**
  The Badger game is an extortion scheme often perpetrated on married men, in whom the victim or “mark” is deliberately coerced into a compromising position then threaten with public exposure of his acts unless blackmail is paid.

- **Bait Car**
  A bait car is a generic term used for a vehicle use by law enforcement agency to capture car thieves. The vehicles are specially modified, with features including GPS tracking, hidden cameras that record audio/video, time, and date, and the ability to remotely monitor a variety of vehicle sensors and to control a vehicle by disabling the engine and locking the doors. The practical does not violate entrapment laws, since suspects are not persuaded to steal the vehicle by any means other than its availability and their own motivation.

- **Call Girl**
  A call girl or escort is a prostitute who is not visible to the general public, like a street walker, and who does not usually belong to an institution like a brothel. One must summon her, usually by calling a telephone number—hence the name call girl often, call girl advertise their services in small ads in magazines, although an intermediary such as an escort agency pimp of pander may be involved. Sometimes the police carryout a sting operation: a police officer, posing as a client, summons a call girl to a hired hotel room, or as a call girl, summons a prospective client. In India, this was done in May 2004; for the first time a prostitution ring using Internet to solicit customers was raided.

- **Operation Pin**
  Operation pin is an initiative of the virtual Global Task Force, which consists of U.K’s national crime squad, the FBI, Interpol, the Royal Canadian Mounted Police and the Australian High tech crime centre. Australian Federal Police (AFP) aim is to identify pedophiles who are using the Internet access child pornography.
- **Cops in shops**

  Cops in shops are an alcohol law enforcement program in the United States in which undercover police officers work with participating alcoholic beverage retailers. The purpose of the program is to discourage minor and adults under the age of 21 from buying alcohol. The program is funded by the century council, an organization that works to reduce under age drinking and drunken driving.\(^\text{90}\)

- **Operation Century**

  Operation century was the code name for a sting operation for investigating a triple murder at Rettendon (Essex, England) Essex police constabulary in 1995. It was assisted by Royal Ulster Constabulary Special Brand Officers. The purpose of this operation was to bring pressure to bear on persons whom they suspected of having knowledge to disclose about the triple murder that would incriminate the suspects in question and or others.\(^\text{91}\)

  In India ever since Tehelka made news capturing corrupt politicians and army officers in the TV camera, sting operations by TV channels seemed to be on the increase. The latest one is the sting operation involving the Hindi Film Actor, Villain, Shakti Kapoor.

  Here is a list of some operations led by Tehelka and others\(^\text{92}\):

  - **Operation Fallen Heroes**

    Tehelks’s modus operandi was to send Manoj Prabhakar to meet players and officials with a hidden camera. Prabhakar would raise the subject of match fixing and hope that the other party would cough up some juicy details.

  - **2000-Operation Gentleman**

    Spread over seven cities and involving over 300 officials which back up from the central Bureau of investigation, this operation targeted cricketers from all ages.

  - **2001- Operation West End**

    sting operation by Tahelka Journalists Aniruddha Bahal and Mathew Samuel Produced a video that showed several members of the Indian
government including the then ruling party BJP’s president Bangaru Laxman accepting bribes to approve defence contracts.

- **2005 - Operation Duryodhana**
  A cobra posts (Aniruddha Bahal) and Aaj Tak Investigation unearthed 11 MPs accepting cash to table questions in the Indian parliament.

- **2005 - Casting Couch**
  India TV sent a woman reporter posing as a struggling actor to trap Shakti Kapoor and Aman Verma to prove the prevalence of the casting couch in bollywood.

- **2005 - Bhaiya Bole**
  India TV caught three legislators of different parties in sexual act with women. However, the channel was sued for showing obscene content on TV and the MP’s charged that all the footage was ‘morphed’.

**2006 - Operation Water Rat**
CNN- IBN smuggled explosives in to Mumbai to show gaping holes in the security apparatus.

**2007 Operation Kalank**
The truth about Gujarat 2002, Tahelka reporters got first hand account from the men who plotted and executed the genocide. This also removed all doubts about the involvement and cover up initiated by the Modi government.93

**India’s Approach to sting operation**
In India we have no specific law which governs such operation and we have no judicial pronouncements till today which guides such operations or the acts of the media. But a person can go to the court under different laws to protect his rights and freedom. We have wiretapping which is a part of sting operation is regulated under the Indian Telegraph Act of 1885.94 In 1996 decision by the Supreme Court95 which ruled that wiretaps are a “serious invasion of an individual Privacy.” The court also laid down guidelines for wiretapping by the government, which define who can tap phones and under what circumstances. Only the Union Home Secretary, or his Counterpart in the State, can issue an order for a tap. The government is also required to show that
the information sought can not be obtained through any other means. The court mandated the development of high level committee to review the legality of each wiretap. Tapped phone calls are not accepted as primary evidence in Indian Courts. Apart from the common law, the Supreme Court has recognized a constitutional origin as well. So firstly, a private action for damages may lie for an unlawful invasion of privacy under the law of torts. These sting operations also violates right to privacy which according to the Supreme Court is guaranteed under Article 21 – right to life and personal liberty. As we are providing that the freedom of expression guarantee in Article 19(1) (a) is not absolute therefore the constitution provides with Article 19(2) which protects the public interest morality and decency. A person who welcomes media interest in his life will not be able to claim a right to privacy as easily as ‘private individual’. There is a vast room for interpretation, especially with terms such as ‘private affairs’ and ‘public Interest’, and interpretation will be made by regulatory authority even through the onus on proving that a particular publication was in public interest lies with the media house. Undoubtedly, the jurisprudence of the Supreme Court will certainly influence interpretation. The Apex court has always upheld the importance of an informed citizenry. ‘A sting operation’ with a genuine motive to create awareness of wrong doing can not prescribed or prohibited.96

In India against the background of some sensational sting operation by media, an official committee has drafted a comprehensive set of guidelines contemplating a series of do’s and don’ts for the broadcast media under which the media person should, identify themselves to potential targets when undertaking such operation.

The broadcasting code and guidelines drafted by a sub committee constituted by the information and broadcasting Ministry, has a separate chapter on news and current affairs which deals in detail on how broadcast journalists should go about their work, including sting operations. The draft seeks to replace the age-old programme and advertising code.
Emphasizing that infringement of privacy in a news based/related programme is important, the guidelines specify that where the media carries out a sting operation, it should be able to justify its under cover operation as “Warranted” in public interest.97

A section titled ‘privacy’ elaborate how a broadcasting service provider (BSP) should avoid any “unwarranted infringement of Privacy” in news based programmes and while obtaining material for such programmes. It spells out a 16 point do’s and don’ts for the media, making it clear that channels must not use material relating to persons personal or private affair or which invades an individuals privacy unless there is an identifiable public interest reason for the material to be broadcast.98

America’s Approach to ‘Sting operation’- The US permits a sting operation only to the federal Bureau of investigation. No private individual, not even a journalist, has the freedom to do so. Even the FBI’s sting operations, are subject to strict ground rules laid down over the years by departmental instructions and ruling of the judiciary.

In many judgment, the US Supreme Court has condemned some FBI sting operations for taking advantage of the naivety, carelessness and negligence of the possibly innocent in order to make them possibly guilty. Even more importantly, privacy international, a Washington-based non governmental organization, has since 1989 been drawing attention to the dangers of an uncontrolled used of clandestine video and audio equipment and closed circuit television. Privacy international system, ‘in a very short time, the systems have challenged some fundamental tenets of justice and created a threat of surveillance society.’ That is precisely why privacy international had wanted appropriate legislation over the industry of miniaturized audio visual technology. In the United Kingdom, part 2 of the Regulation of investigatory powers Act, 2000 governs under cover operations. The code of practice on the use of covert Human Intelligence sources provides a statutory regime for under cover operation so as to comply with the European Convention on Human Right.99
The carrying out of a sting operation may be an expression of the right to free press but it carries with it an indomitable duty to respect the privacy of others. The individual who is the subject of a press or television ‘item’ has his or her personality reputation or career dashed to the ground after the media exposure. He too has a fundamental right to live with dignity and respect and a right to privacy guaranteed to him under Article 21 of the Constitution.

17th Law Commission in its 200th Report has made recommendations to the centre to enact a law to prevent the media from interfering with the privacy rights of the individuals.

7.5 Recapitulation

We are rapidly entering the age of no privacy, where every one is open to surveillance at all times, where there are no secrets from the Government. The aggressive breaches of privacy by the Government increase with geometric proportions. “Wiretapping” and “bugging” run rampant, without effective judicial or legislative control. Secret observation booths in government offices and closed television circuits in industry, extending even to rest rooms, common; offices, conference rooms, hotel rooms and even bed rooms are “bugged for the convenience of government. Federal agents are often wired so that their conversations are either recorded on their persons or transmitted to tape recorders some blocks away....They have broken and entered homes to obtain evidence.....The dossiers on all citizens mount in number and increase in size. Now they are being put on computers so that by pressing one button all the miserable, the sick, the suspect, the unpopular the off-beat people of the nation can be instantly identified.

The significance of the right to privacy has enormously increased in the present social set-up as a rapid development in the field of technology and communication which has vested us with numerous sophisticated electronic and computer devices that have increased the chances of direct and indirect intrusion in the area of an individual’s privacy. Camera cell phones, mini cameras, mini microphones and other surveillance devices are just enemies of right to privacy as they are being used and would also be used in future to
maintain a check over the right to privacy of citizens. A computer can store hundreds and thousands of most personal information of which one may remain quite unaware. Today a sensitive microphone can record even whispering from quite a long distance and one would never come even to realize this fact.

In India media has played a critical role for stirring up the conscience of the people, and bringing forth evil in the society. Media has achieved great heights with the latest technology and it has become a cardinal part in the lives of everyone. Today the absence of media in our lives is something next to impossible. The presence of media in our society assures us of justice in every way. A common man can distrust government but not the media. Hence any finger raised over media puts a question over our democracy too.

Advancing technology enabled the media to make even more searching intrusions into the individual privacy and reach of the television with the assistance of satellite. The advent of miniaturized audio and video technology, specially the pinhole camera technology, enables one to clandestinely make a video/audio recording of conversation and actions of individuals. In India, the media has been first to grab this state of the art technology to conduct 'sting operations' to expose an offence before the police or the judiciary takes the cognizance of the matter. The phrase ‘sting operation’ illuminates the impact of secret media coverage on a person’s reputation by creating a wide spread perception of guilt regardless of any verdict in a court of law. In India, in the absence of law regulating the sting operations, the media has violated and distorted the rules of natural justice and particularly the basic fundamental right of right to privacy enshrined under Article 21 of the Constitution.

This view gaining currency is that “invasion of privacy” can not be condoned and the Government ought to have some mechanism to address such cases, Union Information and Broadcasting Ministry is considering a regulatory mechanism to protect the privacy of individuals.
17th Law Commission in its 200th Report has made recommendations to the centre to enact a law to prevent the media from interfering with the privacy rights of the individuals.
Notes & References:

1. Surveillance from wikipedia, the free encyclopedia E:\ surveillance - wikipedia, the free encyclopedia. Html.
5. Ibid.
6. Keystroke loggers are used for Keystroke logging, which is a method of capturing and recording user Keystrokes.
7. A Sniffer is a piece of software that grabs all of the traffic flowing into and out of a computer attached to a network.
8. A honey pot is a trap set to detect, deflect or in some manner counteracts attempts at unauthorized use of information system.
11. The Indian Telegraph Act, 1885, (Act No. 13 of 1885).
12. Section 5(2) of the Indian Telegraph Act, 1885.
20. Ibid.
24. Id. Pp. 42, 43
25. Ibid.
27. Executive Chartered Secretary, June 2005 privacy protection on the Internet: Legislation and Techniques used in select countries by Madan Lal Bhasin, Head Accounting Department, Mazoon College, Muscat, Sultanate of Oman.
30. Supra Note 29 p. 213.
32. India Gets its First cyber convict, Hindustan Times , 06 February 2003.

34. Id at 215.

35. See http://search security. Techtarget. coms/definition/o,,sid1.4-gci 211838.00 html.

36. See Infra Note 58.


38. Section 43(b) of the Information Technology Act, 2000.

39. Section 43(c) of the Information Technology Act, 2000.

40. Section 43 (i) of the Information Technology Act, 2000.

41. The GIF stands for Graphics Interchange format and is one of the two most common file formats for graphic images on the world wide web. The other is the JPEG. On the web and elsewhere on the internet (for example, bulletin board services) the GIF has become a defects standard form of image.

42. Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put in some one’s computer to secretly gather information about the user and relay it to advertiser or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program. Date collecting programs that are installed with the users knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.

43. See, http://search web services.techtarget.com/s Definition /0 sid 26-gci 341290,00 html.

44. Supra Note 37, at 569.

45. Section 43 (b), 43(c) of the Information Technology Act 2000.

46. Supra Note 28 at p. 218.
49. See http://Search security, techtarget. Com/s Definition/o, s.d 14-gc/213221,00 html.
51. Ibid.
54. Supra Note 47 at p.64.
58. Section 43 (d), (e) and (f) of The Information Technology Act, 2000.
59. Supra Note 29 at 173.
60. Ibid.
62. All India Reporter January 2009 vol. 96 part 1141 at Journall.
65. Black stone commentaries (1765) vol. 4 at pp. 151-152.
68. M.S.M. Sharma v. Srikrishna, All India Reporter 1959 SC, p. 395


71. AIR 1986 SC 515.


74. ‘Nalini Rajan’ “21st Century Journalism in India” First published in 2007 at p. 133.

75. Id p. 134.

76. Ibid.


78. AIR 1995 SC P. 264.

79. Ibid.

80. Ibid.


82. AIR 2008 Madras 244.


84. Ajay Dash, “Sting Operation by media”, discovery publication 1st published 2007 at p.27.

85. Investigative Journalism-wikipedia, the free encyclopedia.

86. Sting operation-wikipedia, the free Encyclopedia June 2007.

87. Supra Note 84 at p.2.

88. Ibid.

89. Ibid.

90. Ibid.
91. Ibid.

92. Ibid.


94. Anand Kumar (student), Symbiosis Law School, Pune, Sting operation— to be or not to be at www.articlebase.com.

95. People Union for civil liberties v. Union of India AIR 1997 SC 568.

96. Supra Note 94.

97. Supra Note 93 at pp.26-27.

98. Id. at pp. 198, 199.


100. 17th Law Commission of India 200th report, 31st August 2006 on “Trial by media: free speech Vs. Fair Trial under CrPC.”