CHAPTER-5

PRIVACY OF COMMUNICATIONS

A. Privileged Communication

B. Telephone-tapping

C. Photography and Publishing

D. Computers

CHAPTER-5

PRIVACY OF COMMUNICATION

The private communication and protection thereof is another important area in relation to the right to privacy. The legal rules under different laws which accord protection to communications made between some parties have been analysed here. The legal provisions protect the privileged communication, however, it does not provide an absolute shield. With the development of science and technology various modes have evolved to peep into private life like, bugging mechanisms, telephone tapping and different photography mechanisms. The computer has been the latest hazards in unveiling the privacy of the individual. Although there is need to develop adequate safeguards in these areas, the available legal provisions have been discussed here.

A. Privileged Communication.

The greatest threat to civilised social life would be a situation in which each individual was utterly candid in his communications with others, saying exactly what he knew or felt at all times. Among mature persons all communication is partial and limited, based on the complementary relation between reserve and discretion.[1] Privacy for limited and protected communication has two great aspects. First, it provides the individual with the opportunities he needs for sharing confidences and intimacies with those he trusts – spouse, "the family", personal friends, and close associates at work. The individual discloses because he knows that his confidences will be held, and because he knows that breach of confidence violates social norms in a civilised society.[2] "A friend" said Emerson [3], "is someone before.....whom I can think aloud". In addition, the individual often wants to secure counsel from persons with whom he does not have to live daily after disclosing his confidences. He seeks professionally objective advice from persons whose status in society promises that they will not later use his distress to take advantage of him. To protect freedom of limited communication, such relationship – with doctors, lawyers, ministers, psychiatrists, psychologists, and others – are given varying but important degrees of legal privilege against forced disclosure. The privacy given to the religious confessions in democratic societies is well known, but the need for confession is so general that

---

1. Alan F. Westin, *Privacy and Freedom*, Atheneum, New York (1970), 37.

2. *Ibid*, at 38.

3. Ralph Waldo Emerson, "*Friendship*", *The complete Works of Ralph Waldo Emerson*, New York (1903), 202.

those without religious commitment have institutionalized their substitute in psychiatric and counseling services [4].

In its second general aspect, privacy through limited communication serves to set necessary boundaries of mental distance in interpersonal situations ranging from the most intimate to the most formal and public. In marriage, for example, husbands and wives need to retain islands of privacy in the midst of their intimacy if they are to preserve a saving respect and mystery in the relation. These elements of reserved communication will range from small matters, involving management of money, personal habits, and outside activities, to the more serious levels of past experiences and inner secrets of personality. Successful marriages usually depend on the discovery of the ideal line between privacy and revelation and on the respect of both partners for that line. In work situations, mental distance is necessary so that the relations of superior and subordinate do not slip into an intimacy which would create a lack of respect and an impediment to directions and connections. Thus, physical arrangements shield superiors from constant observation by subordinates and social etiquette forbids conversations or off-duty contacts that are "too close" for the work relationship. Similar distance is observed in relations between professor and student, parent and child, minister and communicant, and many others. Psychological distance is also used in crowded settings to provide privacy for the participants of group and public encounters; a complex but well understood etiquette of privacy is part of our social scenario [5]. Bates remarked that "we request or recognise withdrawal into privacy in facial expressions, bodily gestures, conventions

---

4. Westin, *Priavcy and Freedom*, 1970, 38.

5. Ibid, 38

like changing the subject, and by exchanging meaning in ways which exclude others present, such as private words, jokes, winks and grimaces".[6] We learn to ignore people and to be ignored by them as a way of achieving privacy in subways, on streets, and in the "non-presence" of servants or children. There are also social conventions within various sub-groups in the population establishing fairly clearly the proper and improper matters for discussion among intimates, workmates, persons on a bus, and other groups.[7]

The organisations need to communicate in confidence with its outside advisers and sources of information and to negotiate privately with other organisations corresponds to the individual's need for protected communication. One aspect of privacy for confidential communication involves the information that organisations acquire from individuals and from other organisations. Private agencies such as life-insurance companies, credit bureaus, employees, and many others collect reams of personal information, sometimes under the compulsion that the benefits offered by the organisation cannot be had unless the information is provided. Government departments, in their capacities as law-enforcement, regulatory, money-granting and employment agencies, collect even more personal data and much of this too is compelled – by a legal duty to respond to the government enquiry. But organisations also need to protect such information against many of the claims to access made by the press and other private and public agencies if they are to continue to get frank and full information from reporting sources. This

---

6. Alan Bates, " Privacy - A Useful Concept?" 42 *Social Forces,* 429, 432 (1964).

7. Alan F. Westin, *Ibid*, note 1 at 39. 12. *Ibid*, at 1814.

fact makes confidential treatment of the data an independent organisational need, not an assertion of privacy solely on behalf of those furnishing the information. [8]

Many private organisations have developed confidentiality policies to govern this issue. Government usually tries to safeguard confidential information through statutes or regulations prohibiting unauthorised disclosures by government employees of information acquired in their official capacities or contained in government files. Pressures on the privacy of governmentally obtained data arise when business, the press, or other governmental agencies claim the right of the people to have access to such information, creating an important area of struggle over executive privacy. [9]

Another aspect of confidential communications involves the privacy of negotiations among organisations in society. Leading examples are labour-management negotiations over working terms, negotiations among political parties and factions over political affairs and the bargains struck by civic groups of all kinds on matters of community relations. Unless the representatives of the negotiating organisations can debate and work toward such bargains in privacy, without premature exposure either to their respective memberships or to the general public, there cannot be a successful process of accommodation and compromise. Privacy is a necessary element for the protection of organisational autonomy, gathering of information and advice, preparation of positions, internal decision-making, inter-organisational negotiations, and timing of disclosure. Privacy is thus not a luxury for organizational life; it is a vital

---

8. *Ibid*, at 49-50.

9. *Ibid*, at 50.

lubricant of the organisational system in free societies. [10]

Privacy of communication received legal protection in India under Sections 121 - 132 of the Indian Evidence Act, 1872. It will not be out of place here to give a brief survey of these sections. Section 121 refers to the privilege of persons connected with the administration of justice. It is against public policy or expediency to allow disclosure of matters in which judges or magistrates have been judicially engaged. Section 121 enacts that a judge or magistrate cannot be compelled to answer questions: (1) as to his own conduct in court as judicial officer; and (2) as to anything which came to his knowledge in court as such judicial officer, unless ordered by a superior court. The privilege does not extend to other collateral matters or incidents occurring in his presence while acting as a judicial officer.[11]

Husbands and wives are competent witnesses in all civil proceedings; and in criminal proceedings against an accused, his or her wife or husband is a competent witness, whether for or against. Section 122 contains a rule of privilege protecting the disclosure of all communications, between persons married to one another, made during marriage, except in certain cases, i.e., in litigation between themselves. The provisions of the section may be summarized thus:

1) The privilege extends to all communications made to a person during marriage, by any person to whom he or she has been married, but not to communications before marriage.

---

10. *Ibid*, at 51.

11. Sudipto Sarkar and V. R. Manohar, *Sarkar on Evidence*, 14th Ed., 1993, Vol 2, 1809.

2) The communication need not be confidential. The rule applies to communications of every nature.

3) The rule of privilege applies equally whether or not the witness or his or her spouse is a party to the proceeding. It extends to all cases, i.e., to cases between strangers as well as to suits or proceedings in which the husband or wife is a party.

4) The privilege extends to communications made to a spouse and not to those made by a spouse. But the privilege is conferred not on the witness (unless the witness happens to be the spouse who made the communication), but on the spouse who made the communication; the witness cannot therefore waive it at his or her own will, nor can the court permit disclosure even if he or she is willing to do it. It is only the spouse who made the communication or his or her representative in interest who can consent to give up the privilege. [12]

Disclosure of secret information contained in unpublished state papers, are privileged from production on the ground of public policy or as being detrimental to the public interest or service. On grounds of public policy, relating to affairs of state contained in unpublished official records are protected from disclosure except with the permission of the head of the department concerned. Section 123 prohibits the disclosure of any evidence derived from unpublished official records relating to any affairs of state without the permission of the head of the department concerned, who has discretion to give or refuse such permission. [13]

---

12. *Ibid*, at 1814.

13. *Ibid*, at 1823.

As in Section 123, public policy also requires that communications made to a public officer in "official confidence" should not be disclosed for being detrimental to the public interest or service. The communication may be oral or in writing. The confidence reposed may be express or implied. Section 124 is not confined to unpublished records as is Section 123. Unlike Section 123, the discretion as to whether disclosure should be made rests with the public officer to whom the communication is made in official confidence and not with the head of the department. The only ground on which privilege may be claimed is prejudice to public interest. [14]

Section 125 entitles a police officer to refuse to disclose the source of his information as to the commission of any offence. On grounds of public policy, the source of information of offence against the laws should not be divulged. If the names of the informers and the channel of communication are not protected from disclosure, no one would be forthcoming to give such information. This privilege is necessary for creating confidence and offering encouragement to informants. It is the duty of every citizen to communicate to his government any information which he has of the commission of an offence against the laws. To encourage him in performing this duty without fear of consequences, the law holds such information to be among secrets of state. Courts of justice, therefore, do not compel or allow the discovery of such information, either by the subordinate officer to whom it is given or by any other person, without the permission of the government.[15]

Sections 126-129 deal with the law relating to professional

---

14. *Ibid*, at 1845.

15. *Ibid*, at 1851.

communications between clients and legal advisers or their clerks. A lawyer is under a moral obligation to respect the confidence reposed in him and not to disclose communications which have been made to him in professional confidence, i.e., in the course and for the purpose of his employment, by or on behalf of his clients, or to state the contents of conditions of documents with which he has become acquainted in the course of his professional employment, without the consent of his client. Section 126 gives legal sanction to this obligation.[16] The privilege given by Section 126 to legal advisers is, by the provisions of Section 127, extended to interpreters and the clerks or servants of barristers, pleaders, attorneys, and vakils. As it is not possible for lawyers to transact all their business in person and they have to employ clerks or agents, the privilege necessarily extends to facts coming to their knowledge in the course of their employment. The protection extends to all the necessary organs by which such communications are effected and therefore an interpreter, or an intermediate agent is under the same obligations as the legal adviser himself. [17]

The privilege is the privilege of the client and not of the legal adviser, and therefore he alone can waive it. Section 126 permits disclosure when it is waived expressly. Section 128 refers to implied waiver; and says that the privilege is not waived if a party to suit gives evidence therein at his own instance or otherwise. Section 128 further says that the privilege is not also lost by merely calling the legal adviser as a witness unless a party questions him on the particular point. [18]

---

16. *Ibid*, at 1857.

17. *Ibid*, at 1877.

18. *Ibid*, at 1877-78.

Sections 126, 127 and 128 prevent a legal adviser or his clerk, servant, etc., from disclosing confidential communications made in the course of professional employment. By Section 129 a similar protection is afforded to the client which says that no one shall be compelled to disclose confidential communication which has taken place between himself and his legal adviser, unless he himself offers as a witness ; in which case he can be compelled to disclose any such communication which the court thinks necessary to explain the evidence which he has given, but no others. [19]

Section 130 lays down that a witness who is not a party to a suit, i.e., a stranger, shall not be compelled to produce (1) his title-deeds or documents in the nature of title- deeds, e.g., documents of pledge or mortgage, or (2) any document the production of which might tend to criminate him, unless he has agreed in writing to produce them. The reason for the rule is protection from the mischief and inconvenience that might result from compulsory disclosure of title. Section 131 prohibits the production of document in the possession of a person, which any other person would be entitled to refuse to produce if they were in his possession. [20]

Under Section 132 a witness cannot refuse to answer a question which is relevant to the matter in issue in any suit or in any civil or criminal proceeding simply on the ground that the answer will tend to criminate him or expose him to a criminal charge, penalty or forfeiture. The legislature, while depriving the witness of the privilege has in order to

---

19. *Ibid*, at 1879.

20. *Ibid*, at 1883.

remove any inducement to falsehood, added a proviso to the section declaring that if a witness is compelled by the court to answer, such incriminating answers will not subject the witness to any arrest or prosecution or be proved against him in any criminal proceedings except in case of a prosecution for giving false evidence. [21]

During the last few years, courts have started giving protection against the disclosure or misuse of confidential information. In the beginning, injunction was the remedy ordinarily sought in such cases. However, one can now see a definite trend recognising the right of the aggrieved individual to claim damages also, where there is unauthorised disclosure or use of information which was imparted in confidence. Even though many of these cases were concerned with trade secrets mainly, they do not rest merely on the element of monetary gain or loss. In fact, some of them reflect protection of confidence in the sphere of personal privacy. [22]

As early as 1846, in the case *Prince Albert* vs. *Strange*,[23] an injunction was obtained against the unauthorised circulation of certain etchings privately made by Queen Victoria and her Prince Consort.

In 1967, in *Argyll* vs. *Argyll*,[24] an injunction was obtained by a wife against her husband, who was about to disclose certain confidential matters communicated to him by the wife, the disclosure having been thought of by her husband after the marriage had broken down. In this

---

21. *Ibid*, at 1891.

22. P.M. Bakshi, Breach of Confidence as an Actionable Wrong, *Chartered Secretary*, (1998), 11.

23. (1848) 2 De. & Sm. 652.

24. (1967) Ch. 302.

case it was held that with the object of preserving the marital relationship, it was the policy of the law that communications, not limited to business matters, between husbands and wife should be protected against breaches of confidence, so that, where the court recognised that such communications were confidential and that there was a danger of their publication within the mischief, which it was the policy of the law to avoid, it would interfere; and that, on the facts, publication of some of the passages complained of would be in breach of marital confidence. It was further observed that, it being the policy of the law to preserve the close confidence and mutual trust between husband and wife, subsequent adultery by one spouse resulting in divorce did not relieve the other spouse from the obligation to preserve their earlier confidences. Accordingly, the plaintiff's adultery did not entitle the first dependant to publish the confidences of their married life, and an injunction would be granted restraining him from doing so.

From the aforesaid discussion, it can be surmised that if certain information or other material has been obtained in confidence, and is published wrongfully, action for damages for breach of confidence would lie. In appropriate cases, injunction is also available. Except where there are overriding considerations of public interest, where a person obtains information in the course of a confidential employment, the law does not allow him to make any improper use of the information so obtained. [25]

The essence of this branch of law is the principle that a person who has obtained information in confidence is not allowed to use that information as a "springboard" for the purpose of activities detrimental to the person who made the confidential communication. In *Saltman*

---

25. *Pollard* vs. *Photography* Co. (1889) 40 Ch. D. 345.

Engineering Co. vs. *Campbell Engineering Co.*,[26] certain drawings were entrusted by the plaintiff to the defendant, for the purpose of manufacturing tools for making leather pouches. The defendants made use of the drawings in order to make leather pouches on their own account. The court held such use to be illegal. As the plaintiff had not given his consent to such use he was entitled to an injunction. The Court of Appeal made it clear that contract or no contract, the obligation arose from the circumstances.

It may be noted here that the question of confidence, apart from the breach of copyright or patent, has occasionally arisen in India also. In a Delhi case, *John Richard Brady* vs. *Chemical Process Equipment,*[27] the plaintiff imparted to the defendant know-how (also giving certain drawings and other technical documents). This was held to have given rise to a confidential relationship. The Court issued an injunction to prevent abuse of the drawings. It was found that defendant's machine was strikingly similar to the drawings given by the plaintiff. The Delhi High Court quoted the following passage from Patrick Heirn, *Business of Industrial Licensing,* pages 112-115 :

> "The maintenance of secrecy which plays such an important part in securing, to the owner of an invention, the uninterrupted proprietorship of marketing *know- how,* which thus remains at least a form of property, is enforceable at law."

---

26. (1948) 65 R.P.C. 203 (CA)

27. (1987) 13 *Ind .Jud. Reports* (Del) 739.

B. Telephone Tapping

The conditions of modern living, with close proximity of dwellings and people, rapid transportation, easy communication, and not least, the developments of modern technology, have gravely accentuated the problem of retaining a reasonable area of privacy for the individual. The modern eavesdropper is able not only to report on us, but with the assistance of science, can actually reproduce our very words as spoken with all their nuances, tones, and individual characteristics. The problem of the eavesdropper who is ready to invade the privacy of others, either for his personal gain or out of a sense of public duty, has probably always been with us. The eavesdropper of old did not present a major problem to society, for it was possible to guard against his presence. With the invention of the telegraph and telephone and their quick acceptance as indispensable means of communication, however, the problem of the eavesdropper assumed new magnitude. No longer the person spied upon needed to be within listening distance. The devices of science could now be utilized to facilitate the task of the eavesdropper, who might be far removed from his victim physically and yet be able to maintain surveillance as efficiently as if he were hidden in the kitchen closet. Eavesdropper did not wait long to capitalize on the invention of the telegraph, and interception of transmitted messages became a prevalent practice. [1]

One of the earliest cases where the American Supreme Court dealt with the constitutional question raised by wire tapping was *Olmstead* vs.

---

1. Jacob W. Landynski, *Search and Seizure and the Supreme Court – A Study in Constitutional Interpretation*, 1966, 198-99.

United States, [2] decided in 1928. The *Olmstead* case is considered a landmark in constitutional law, not so much for the decision itself as for the quality of its oft quoted dissenting opinions.

Chief Justice Taft in his opinion for the Court rejected the contention that wire tapping was a search under the Fourth Amendment. "There was no searching.....the evidence was secured by the use of .....hearing and that only," said Taft. "There was no entry of the houses or offices of the defendants." [3] Nor could the interception of a conversation qualify as a seizure under the Fourth Amendment, for the Amendment referred only to the seizure of tangible items. Moreover, one who uses a telephone is in communication with someone who is outside the house: "The language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office." [4]

Even if the Fourth Amendment did not render wire tapping a search in the constitutional sense. Olmstead contended that the evidence was nevertheless inadmissible as having been obtained in violation of law which made wire tapping a criminal offence. The Chief Justice rejected this argument by limiting the application of the federal exclusionary rule to violations of the Constitution. In a passage which revealingly summed up the majority's philosophy and its low esteem of the exclusionary rule, he said: " A standard which would forbid the reception of evidence if obtained by other than nice ethical conduct by government officials would

---

2. 277 U.S. 438 (1928).

3. *Ibid*, at 464.

4. *Ibid*, at 465.

make society suffer and give criminals greater immunity than has been known heretofore." [5]

Justice Holmes' dissent is one of his best-known opinions because of his characterization of wire-tapping as "dirty business".[6] Actually, Justice Holmes was referring not to wire-tapping itself but to illegal wire-tapping. Indeed, he was "not prepared to say that the penumbra of the Fourth and Fifth Amendments covers the defendant"[7] and he addressed himself exclusively to the moral issue involved, that is, whether evidence secured in violation of law should be admissible. Justice Holmes thought not.

Justice Brandeis also had some strong words to say on the moral issue, but, unlike Holmes, he was unequivocal in his assertion that wire-tapping was a search within the meaning of the Fourth Amendment. In words that today seem to be almost prophetic; he painted a grim picture of the probable consequences to privacy of the new technology if the protection of the Constitution could not be invoked to cope with this development:

> "Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet ..... The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be

---

5. *Ibid*, at 468.

6. *Ibid*, at 470.

7. *Ibid*, at 469.

developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions "[8].

Turning to the moral issue which had agitated Justice Holmes, Justice Brandeis agreed that, regardless of the constitutionality of wire-tapping, evidence obtained by this method should be held inadmissible when obtained, as in this case, in violation of law.

In *Katz* vs. *United States*, [9] it was held by the American Supreme Court that the attaching by FBI agents, of an electronic listening and recording device to the outside of a public telephone booth from which a suspect placed his call, constitutes a violation of the Fourth Amendment's prohibition of unreasonable searches and seizures, in the absence of an antecedent order judicially sanctioning such surveillance.

Thus the initial view of the American Supreme Court in *Olmstead* vs. *United States* [10] that the Fourth Amendment had no application to telephone-tapping was modified in *Katz* vs. *United States* [11] to the effect that the Court extended it to protect the privacy against bugging.

In *United States* vs. *Nixon,*[11a] following the indictment of seven high-ranking White House officials, including former special presidential assistants H.R.Halderman and John Ehrlichman and former Attorney

---

8. *Ibid*, at 473-74.

9. 389 U.S. 347 (1967).

10. (1928) 72 L. Ed. 944.

11. (1967) 19 L. Ed. 2d. 576.

11a. 418 U.S. 683.

General John Mitchell, for conspiracy to defraud the US Government and obstruction of justice, the special prosecutor obtained a subpoena directing President Richard M. Nixon to deliver to the trial judge certain tape-recordings and memoranda of conversation held in the White House. The trial judge would then examine those tapes and documents and give to the prosecution and defence those portions relevant to the issues at trial. The remainder would be returned to the President. Nixon produced some of the subpoenaed material but withheld other portions, invoking executive privilege, which he claimed, placed confidential presidential documents beyond judicial control. The trial judge denied the President's claim and he appealed to the Court of Appeals. The special prosecutor asked the Supreme Court to review the case before the Court of Appeals had passed judgment and the Justices agreed.

Neither the doctrine of separation of powers, nor the need for confidentiality of high level communications, can sustain an absolute, unqualified presidential form of immunity from judicial process under all circumstances. The President's need for complete candour and objectivity from advisers calls for great deference from the courts. However, when the privilege depends solely on the broad, undifferentiated claim of public interest in the confidentiality of such conversations, a confrontation with other values arises. In the absence of a claim of need to protect military, diplomatic, or sensitive national security secrets, we find it difficult to accept the argument that even the very important interest in confidentiality of presidential communications is significantly diminished by production of such material *in camera* with all the protection that a district court will be obliged to provide.

The expectation of a President to the confidentiality of his conversations and correspondence, like the claim of confidentiality of

judicial deliberations, for example, has all the values to which we accord deference for the privacy of all citizens and added to those values, the necessity for protection of the public interest in candid, objective, and even blunt or harsh opinions in presidential decision-making.... These are the considerations justifying a presumptive privilege for presidential communications. The privilege is fundamental to the operation of Government and inextricably rooted in the separation of powers under the Constitution. Nowhere in the Constitution is there any explicit reference to a privilege of confidentiality, yet to the extent this interest relates to the effective discharge of a President's power, it is constitutionally based.

There is no express guarantee against tapping of telephone under the Constitution of India, therefore, the argument that, it violates the privacy of conversation under Article 21 was raised before the Court in *R. M. Malkani* vs. *State of Maharashtra* .[12] In this case, one of the contentions of the appellants was that the evidence was illegally obtained in contravention of Section 25 of the Indian Telegraph Act and therefore the evidence was inadmissible. Section 25 of the Indian Telegraph Act, 1885 states that if any person intending to intercept or to acquaint himself with the contents of any message damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other thing whatever, being part of or used in or about any telegraph or in the working thereof he shall be punished with imprisonment for a term which may extend to three years, or with fine or with both [13].

---

12. AIR 1973 SC 157.

13. Telegraph is defined in the Indian Telegraph Act in Sec 3 to mean any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals,

The Court held that where a person talking on the telephone allows another person to record it or to hear it, it cannot be said that the other person who is allowed to do so is damaging, removing, tampering, touching machinery, battery line or post for intercepting or acquainting himself with the contents of any message. There was no element of coercion in attaching the tape recorder to the telephone. There was no violation of the Indian Telegraph Act. Recognizing the right to privacy of conversation of innocent person, the Court observed:

> "The telephonic conversation of an innocent citizen will be protected by courts against wrongful or high-handed interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servant. It must not be understood that the courts will tolerate safeguards for the protection of the citizen to be imperiled by permitting the police to proceed by unlawful or irregular methods" [14].

The provision empowering the Government to tap telephone under Section 5(2) of the Indian Telegraph Act was challenged by the People's Union for Civil Liberties for being violative of the right to freedom guaranteed under Articles 19(1)(a) and 21 of the Constitution of India in the case of *People's Union for Civil Liberties* (*PUCL*) vs. *The Union of India and Another*,[15] popularly known as the 'Telephone-tapping case'. The writ petition was filed in the wake of a report 'Tapping of

---

writing, images and sounds or intelligence of any nature by wire, visual or other electromagnetic emissions, radio waves or Hertizan waves, galvanic, electric or magnetic means.

14. AIR 1973 SC 157, 164.

15. AIR 1997 SC 568.

Politicians' Phones by the Central Bureau of Investigation (CBI)' which appeared in the `Mainstream` dated March 26, 1991. Section 5(2) of the Indian Telegraph Act of 1885, which was at the core of the controversy, provides that on the occurrence of any public emergency, or in the interest of public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government, may, if satisfied that it is necessary or expedient to do so in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

Therefore, Section 5(2) permits the interception of messages in accordance with the provisions of the said section. "Occurrence of any public emergency" or "in the interest of public safety" are the *sine qua non* for the application of the provisions of Section 5(2). Unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers under the said

section.[16]

Kuldip Singh, J., delivering the judgment observed:

"Telephone-tapping is a serious invasion of an individual's privacy. With the growth of highly sophisticated communication technology, the right to hold telephone conversation, in the privacy of one's home or office without interference, is increasingly susceptible to abuse, It is no doubt correct that every Government, howsoever democratic, exercises some degree of *sub rosa* operation as a part of its intelligence outfit but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day".[17]

The Court further observed that the right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts of a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by Law" [18] It was observed that the right to privacy, by itself, has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy". Conversations on the telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life. It is considered so

---

16. *Ibid*, at 576.

17. *Ibid*, at 570.

18. *Ibid*, at 574

important that more and more people are carrying mobile telephone instruments in their pockets. It was said:

> "Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone-conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution unless it is permitted under the procedure established by law".

The Court also observed that the right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution means the right to express one's convictions and opinions freely by word of mouth, writing, printing, picture, or by any other manner. When a person is talking on the telephone he is exercising his right to freedom of speech and expression. Telephone-tapping unless it comes within the grounds of restrictions under Article 19(2) would infract Article 19(1)(a) of the Constitution.[19]

In the absence of any provision for procedural safeguard in the Telegraph Act in the matter of telephone-tapping, the Supreme Court, in the above case, directed observance of following procedure by way of safeguard before resorting to telephone- tapping:

1. An order for telephone-tapping in terms of Section 5(2) shall not be issued except by the Home Secretary, Government of India and Home Secretaries of the State Governments. In an urgent case the power may be delegated to an officer of the Home Department of the Government of India and the State Governments not below the rank of Joint Secretary. Copy of the order shall be sent to the Review Committee

---

19. *Ibid*, at 574-75.

concerned within one week of the passing of the order.

2. The order shall require the person to whom it is addressed to intercept in the course of their transmission by means of a public telecommunication system, such communications as are described in the order. The order may also require the person to whom it is addressed to disclose the intercepted material to such person and in such manner as are described in the order.

3. The matters to be taken into account in considering whether an order is necessary under Section 5(2) shall include whether the information which is considered necessary to acquire could reasonably be acquired by other means.

4. The interception required under Section 5(2) shall be the interception of such communications as are sent to or from one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications to or from, from any particular person specified or described in the order or one particular set of premises specified or described in the order.

5. The order under Section 5(2) shall unless renewed, cease to have affect at the end of period of two months from the date of issue. The authority which issued the order may, at any time before the end of two month's period renew the order if it considers that it is necessary to continue the order in terms of Section 5(2) of the Act. The total period for the operation of the order shall not exceed six months.

6. The authority which issued the order shall maintain the following records:

a) the intercepted communications,

b) the extent to which the material is disclosed,

c) the number of persons and their identity to whom any of the

material is disclosed,

d) the extent to which the material is copied, and

e) the number of copies made of any of the material.

7. The use of intercepted material shall be limited to the minimum that is necessary in terms of Section 5(2).

8. Each copy made of any of the intercepted material shall be destroyed as soon as its retention is no longer necessary in terms of Section 5(2).

9. There shall be a Review Committee consisting of Cabinet Secretary, the Law Secretary at the level of the Central Government. The Review Committee at the State level shall consist of Chief Secretary, Law Secretary and another member, other than the Home Secretary, appointed by the State Government.

a) The Committee shall on its own, within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under Section 5(2). Where there is or has been an order whether there has been any contravention of the provisions of Section 5(2).

b) If on an investigation the Committee concludes that there has been a contravention of the provisions of Section 5(2), it shall set aside the order under scrutiny of the Committee. It shall further direct the destruction of the copies of the intercepted material.

c) If on investigation, the Committee comes to the conclusion that there has been no contravention of the provisions of Section 5(2) it shall record the finding to that effect [20].

---

20. *Ibid*, at 578-79.

C. Photography and Publishing

A free and unrestrained press has long been recognized as one of the hallmarks of liberty. In fact, Justice Stewart went so far as to equate the press with a fourth branch of government [1] and although the exact scope of the freedom of the press is debatable, most scholars and judges agree that the press serves as an important check on government and a source of information for the people. Despite its acknowledged importance, however, the press, like any other institution, has the potential to abuse its freedom. As James Madison commented "some degree of abuse is inseparable from the proper use of everything, and in no instance is this more true than in that of the press." [2] During a time of tabloid newspapers and exposé television programs perhaps Madison's words ring truer today than ever before. Lately, however it has not been the government that has objected to a cantankerous press, an obstinate press, and a ubiquitous press but rather private individuals who complain of the intrusive, harassing and mercenary tactics of tabloid photographers and who long for a balance between the people's right to know versus a person's right to privacy [3].

This tension was recently exacerbated by the controversy surrounding the role of "paparazzi" photographers in the automobile accident that killed Princess Diana in August 1997. Prompted by public

---

1. *See,* Protter Stewart, Or of the Press, 26 *Hastings L J* 631, 634 (1975)

2. James Madison, *Report on the Virginia Resolutions,* in 4 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 546,571 (Jonathan Elliot ed., 2d ed. 1937)

3. 112 *HLR* 1367 (1999).

outcry over the controversy, members of Congress quickly proposed a new federal legislation to control the press, and the California state legislature was soon to follow with its own legislation. Responding to claims that paparazzi journalists would go to any lengths and use the latest technology to obtain pictures or soundbites, the legislators sought to enhance the penalties for invasion of privacy by creating both civil and criminal actions against people who intrude on others privacy through either conventional or high-tech means. Despite bipartisan support, the 105th congress did not pass the federal bill. The California state legislature however did pass the Senate Bill which became law on September 29, 1998. [4]

As stated earlier, the right to privacy originated in an 1890 article by Samuel Warren and Louis Brandeis, *The Right to Privacy,*[5] which created a minor revolution in the development of the common law. The article criticized the press for "overstepping in every direction the obvious bounds of propriety and of decency" [6] and proposed a new tort for the violation of privacy rights.[7] By 1960, acceptance of this new tort had spread and majority of the states recognized the right of privacy in some form.[8] Since then, the concept of privacy has developed into four distinct torts: unreasonable intrusion upon a persons seclusion; public disclosure of private facts; publicity that places a person in a false light ; and

---

4. *Ibid,* at 1368.

5. Samuel D. Warren & Louis D. Brandeis. The Right to Privacy, 4 *HLR* 193 (1890).

6. *Ibid,* at 196.

7. *See, Ibid,* at 195-97, 214-19. (Discussing the limitations on the right to privacy and what remedies may be granted for enforcement of the right).

8. *See* , William L. Prosser, Privacy, 48 *Cal. Law Rev.* 383,383 (1960)

appropriation of a person's name or likeness.

At the same time, laws prohibiting harassment exist in several states. Whereas the tort of intrusion generally exempts photographers from liability for taking unwanted photographs in or from public places, harassment statutes enable individuals to obtain injunctive relief from persistent press hounding, regardless of where it occurs.

A quarter century ago, for example Jacqueline Kennedy Onassis obtained an injunction from a federal district court against Donald Galella,[9] a freelance celebrity photographer and self-described "paparazzo".[10] According to Onassis, Galella had engaged in a campaign of harassment against Onassis and her family. More recently, in *Wolfson* vs. *Lewis* [11] a couple obtained an injunction against reporters who were working on a story for the television program *Inside Edition.* The Court acknowledged that intrusion claim generally do not arise from matters occurring in public view but held that conduct amounting to persistent harassment and unreasonable surveillance could rise to the level of intrusion upon seclusion. Theories of harassment thus enable individuals to obtain indirect protection of even public expectations of privacy. [12]

In addition to the aforementioned prohibitions on intrusion and harassment, a number of other laws protect individuals from overly aggressive photographers. For example, photographers cannot trespass on private property. Also, assault and battery statutes prohibit photographers

---

9. *See, Galella* vs. *Onassis,* 487 F. 2d. 986, 993 (2d Cir.1973).

10. The term "paparazzo" refers to an obnoxious type of photographer. *See , Ibid,* at 991.

Translated literally, the term means "a kind of annoying insect." *Ibid,* at 991-92.

11. 924 F. Supp. 1413 (E. D. Pa. 1996).

12. Privacy, Photography and the Press 111 *HLR* 1086, 1089.

from engaging in or threatening unwanted physical contact with their subjects. Moreover, photographers who use motor vehicles to chase their subjects risk prosecution for reckless endangerment. These laws protect everyone - not just celebrities and public figures - from overly aggressive photography, and they do so without unduly restricting freedom of speech and expression. [13]

Recently these traditional torts of trespass, harassment, reckless endangerment and others have been invoked with greater frequency, as competitive pressures among the media have created a frenzy in reporters, editors, correspondents and producers to catch a sensational story. Nevertheless, the ability of these torts to protest privacy is questionable, as ever-advancing technology renders "public" those places and activities that were once "private". Thus as Warren and Brandeis realized over 100 years ago, it may be necessary to respond to these "recent inventions and business methods" and to consider "the next step which must be taken for the protection of the person, and for securing to the individual" the right to privacy. [14]

The tort of unreasonable intrusion, which provides a model for the California anti-paparazzi statute "concerns an individual's claim to have a right to a 'personal space', where other citizens and the government are normally not allowed to trespass".[15] The tort protects against both nonconsensual physical intrusions into legally recognized places of privacy and "unwarranted sensory intrusions such as eavesdropping,

---

13. *Ibid*, at 1090

14. Warren & Brandies, *Ibid* note 5, at 195

15. Rodney A. Smolla, *Free Speech in an Open Soceity* 120 (1992).

wiretapping, and visual or photographic spying".[16] A person is liable for unreasonable intrusion when he intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, if the intrusion would be highly offensive to a reasonable person. [17]

To prove the first element of the tort, that an intrusion actually occurred, the plaintiff must have had an objectively reasonable expectation of privacy in the place, conversation or activity upon which the defendant allegedly intruded. In a few jurisdictions, this element is satisfied only if the defendant physically trespassed on property "occupied privately by a plaintiff for purposes of seclusion". Most jurisdictions, however, do not focus the inquiry on the plaintiff's property rights, but instead consider the nature of the relevant place, conversation or activity and its accessibility to the public. If these jurisdictions of the place where the alleged intrusion occurred was accessible to the public or was on private property that was in public view, then the tort generally would not protect the plaintiff's privacy. Therefore, in some situations, the plaintiff, through her own lack of care, can relinquish the privacy provided by private property. [18]

The second element of the intrusion tort, that the defendant intruded upon privacy in a manner highly offensive to a reasonable

---

16. *Ibid,* at 489.

17. Privacy, Technology and the California "Anti-Paparazzi" Statue, 112 *HLR* 1349, 1370.

18. *See, Deteresa* vs. *American Broad. Cos.,* 121 F. 3d 460, 466 (9th Cir. 1997) (finding no intrusion when a reporter secretly recorded a conversation that he had with the plaintiff while standing at the front door of the plaintiff's home, because the plaintiff "spoke voluntarily and free with an individual whom she knew was reporter ") .

person, is generally determined on the basis of all the circumstances of the intrusion, including its degree and setting and the intruder's motives and objectives. When an alleged intruder is a member of the press in pursuit of a news story, his motivations are particularly important to the offensiveness analysis. In such situations, courts have recognized that even though the First Amendment does not immunize members of the press from liability for torts that they commit while gathering news, it does reflect a strong societal interest in effective and complete reporting of events, that may – as a matter of tort law – justify an intrusion that would otherwise be considered offensive. [19]

The fact that courts require a more significant showing of offensiveness when the alleged intruder is gathering news does not, however, give the press *carte blanche* to use whatever technique it deems necessary. Some methods of reporting, such as asking questions, would rarely if ever be deemed an actionable intrusion In contrast, other news gathering activities, such as trespassing into private property or wiretapping someone's telephone could rarely, if ever, be justified by a reporter's need to get the story because these activities would be deemed highly offensive even if the information sought was of weighty public concern. Between these two extremes lie difficult cases, many involving the use of photographic and electronic recording equipment for which tort law provides no bright line. It is precisely this uncertainty that has undermined the effectiveness of the intrusion tort. [20]

Thus, despite over 100 years of development, traditional privacy law is generally considered weak; indeed Mc Clurg remarked that a

---

19. *See,* Ibid, note 17 at 1317.

20. *Ibid,* at 1371-72

"lesson of modern privacy law in the tort arena is that if you expect legal protection for your privacy, you should stay inside your house with the blinds closed".[21] It is said that the modern tort of intrusion is nothing but trespass law updated to the age of potentially intrusive devices.[22] Warren and Brandeis complained of "recent inventions" such as instantaneous photographs and numerous mechanical devices that threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house tops [23] but those devices pale in comparison to modern technology. Today's news gatherers often employ high- powered cameras, hidden cameras that can fit into tie-tacs or clocks, microphones that can pick up sound on the other side of walls or at a distance of up to 100 yards, night- vision scopes, and even satellite photographs. [24] The tort of intrusion has failed to keep pace with these intrusions. [25]

On its face, the tort of intrusion has the potential to reach abuses of

---

21. *See,* Andrew Jay Mc Clurg, Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places, 73 *N.C.L Rev.* 989, 990 (1995).

22. Mark Sableman, *More Speech, Not Less: Communications Law in the Information Age,* 128 (1997).

23. Warren & Brandeis,*Ibid,* note 5, at 195.

24. *See,* Mc Clurg, *Ibid,* note 21, at 1018-21 and 150-176. Although statutes concerning wiretapping and eavesdropping prohibit the use of some of these devices in certain situations, *See,* e.g., 18 U.S.C § 2510-2520 (1994) the statutes nevertheless leave the press with substantial freedom to use many of these devices to gather news surreptitiously, *See,* e.g., *Desnick* vs *American Board Cos.,* 44 F. 3d 1345, 1351-53 (7th Cir. 1995) (finding no violation of wiretapping statutes and no invasion of privacy when reporters used hidden cameras to record their encounters with the plaintiff inside the plaintiffs opthalmic clinic).

25. *See, Ibid.* Note17 at 1372.

technology. The language of the tort includes those intrusions that occur physically or otherwise, which suggests that the tort applies to activities that use technology to achieve the same result as a physical intrusion. Some courts have, on occasion, given the tort this broad definition. For the most part, however, courts have so narrowly limited the tort that it is largely toothless in the face of an increasingly intrusive press. It is difficult to explain courts indifference towards technology. Some courts may tie privacy interests to property interests and refuse to find an intrusion unreasonable if no physical invasion has occurred. This possibility cannot fully account for the weakness of the tort with regard to technology, however as most courts recognize that an intrusion need not be physical in order to be unreasonably offensive. Therefore, court's reluctance to find "technological intrusions" may have more to do with the tort itself. [26]

Intrusion requires a reasonable expectation of privacy in the place, conversation, or activity intruded upon and it requires that the intrusion be highly offensive. The problem with this formulation is that it allows privacy to be diminished as new technology reduces what individuals can reasonably expect to be private, and as social attitudes become more accepting of intrusive uses of technology. Although the case law does not explicitly address this point. It does demonstrate the susceptibility of the common law intrusion tort to technological and social change. In *Shulman* vs. *Group W. Productions, Inc.,* the California Supreme Court distinguished between an accident scene near a freeway, which a reporter could videotape without intruding, and the inside of a rescue helicopter,

---

26. *Ibid,* at 1372-73.

where the plaintiff could have a reasonable expectation of privacy.[27] The difference between the places was that the attendance of reporters and photographers at the scene of an accident is to be expected, but there is no law or custom permitting the press to ride in ambulances without the patient's consent.[28] As this reasoning indicates, the reasonable scope of person's privacy expectation depends partially on the methods of information collection available to the press and public – once the press establishes a law or custom that permits a form of newsgathering that was previously uncommon, then a plaintiff will no longer have a reasonable expectation of privacy with respect to that form of newsgathering. Therefore, by varying the frequency of use of any intrusive newsgathering technique, the media can, "in some sense define the scope of legal protection provided by the intrusion tort." [29]

In *Dow Chemical Co.* vs. *United States,* [30] the US Supreme Court held that the Environmental Protection Agency had not conducted a search for the Fourth Amendment purposes when it flew over the defendant's plant and took pictures with an image- enhancing camera.[31] The Court reasoned that even though "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public....might be constitutionally proscribed absent a warrant", the use of the camera did not raise such problems because it was only "a conventional, albeit precise, commercial camera commonly used in map-

---

27. *See, Shulman*, 995 P. 2d at 490 (Cal 1998).

28. *Ibid.*

29. *See, Ibid*, note 17, at 1374.

30. 476 U.S 227 (1986).

31. *See, Ibid,* at 238 - 39.

making." [32] The court explicitly tied the permissible degree of invasion to the availability of the surveillance technique used, a formulation identical to the approach taken by the California Supreme Court in *Shulman.* Thus both the *Shulman* court and the *Dow Chemical* court defined privacy in terms of what can and does reasonably intrude upon it.

If an individual's reasonable expectation of privacy depends on what can intrude upon it then the new technological innovations can render unreasonable those privacy expectations that were once reasonable. Although no case directly asserts that new technology affects a person's reasonable privacy expectations, contrasting two Ninth Circuit cases suggests that technology does play such a role. In *Dietemann* vs. *Time, Inc.,*[33] the court found an unreasonable intrusion when a reporter used a hidden microphone to record a conversation that he had with the plaintiff inside the plaintiff's home.[34] By contrast, in *Deteresa vs. American Broadcasting Cos.* ,[35] decided twenty-six years after *Dietemann,* the Ninth Circuit found no unreasonable intrusion when a reporter used a hidden microphone to record a conversation that he had with the plaintiff on the front step of her home.[36] The *Deteresa* court distinguished *Dietemann* on the grounds that the reporter never entered Ms. Deteresa's home and the that Ms. Deteresa knew that the person to whom she spoke was a reporter. However, as for the first distinction, Ms. Deteresa's expectation of privacy was not in her home, but rather in her conversation

---

32. *Ibid.* at 238.

33. 449 F. 2d 245 (9th Cir. 1971).

34. *See, Ibid* at 249.

35. 121 F. 3d 460 (9th Cir. 1997).

36. *See, Ibid* at 466.

with the reporter. Therefore a distinction based on the character of the *place*, as opposed to the confidentiality of the *conversation*, seems immaterial considering that both Ms. Deteresa's conversation and Mr. Dietemann's conversation occurred in places where the general public could not hear them. As for the second distinction, the *Deteresa* Court ignored the *Dietemann* court's reasoning a risk that what is heard will be repeated, he "does not and should not be required to take the risk that what is heard... will be transmitted by... (a) recording".[37] The *Deteresa* court, by contrast, stated merely that "Ms. Deteresa spoke voluntarily and freely with an individual whom she knew was a reporter", [38] implying that Ms. Deteresa should have been aware that what she was saying could have been recorded, a risk that Mr. Dietemann did not have to assume. The accessibility of the hidden microphone technology seems to be the only principled distinction that rendered unreasonable for Ms. Deteresa an expectation of privacy that had been reasonable for Ms. Deteresa an expectation of privacy that had been reasonable for Mr. Dietemann . Accordingly the prevalence of the technology apparently diminished the protection provided by the intrusion tort.

Although, the use of new technology plays a role in undermining the intrusion tort, it is probably not solely responsible for the torts decreasing effectiveness. Changing social norms have also contributed to the erosion of the tort. As an initial matter, the public's desire for shocking, titillating and voyeuristic entertainment provides a lucrative market for intrusively gathered information. However, the public's appetite for this type of news and entertainment does more than just

---

37. *Dietemann*, 449 F. 2d at 249

38. *Deteresa*, 121 F. 3d at 466.

provide a market for the media to serve; it also immunizes the media from liability for its intrusive conduct. Because the intrusion tort relies on whether conduct is considered highly offensive, it also directly correlates with society's view about privacy: as concerns about privacy relax, so does the protection the tort provides. Trying privacy to social norms in this manner may be a generally valid way to define such an amorphous concept but it is not without problems. Specifically, much like the effect of changing technology on the reasonableness of a person's privacy expectations correlating privacy with social norms allows intrusions that were once considered highly offensive to become socially acceptable with time. As a result, the intrusion tort is weakened considerably in the face of advancing technology and an increasingly voyeuristic social attitude, leaving personal privacy rarely protected .[39]

Amidst protests that traditional tort law did not sufficiently protect privacy interests the California state legislature passed Senate Bill 262, a bill designed to address a widely experienced problem. The loss of privacy as a result of advancing technological changes. The statute is remarkable not only for its attempt to address the shortcomings of the common law privacy torts, but also for the manner in which it does so. The statute departs from the common law method of protecting privacy, which is to regulate privacy directly by defining it in terms of "solitude", "seclusion" or "private affairs or concerns". Instead, the statute seeks to protect privacy indirectly by improving the protections provided by non-legal forms of regulation. With this approach, the statute attempts to avoid the problems that undermined the common law intrusion tort. [40]

---

39. *See*, *Ibid*, note 17, at 1376.

40. Ibid, at 1376-77.

The California anti-paparazzi statute seizes upon the notion that the law can be used to regulate physical barriers, markets, and norms directly in an effort to protect privacy indirectly. Most importantly, the statute seeks to resurrect the privacy protection traditionally furnished by physical barrier by "redefining" what is meant by physical space : the statute defines a person's private "space" not in terms of feet or yards, but instead in terms of what can be observed without the assistance of sensory-enhancing technology. The statute also imposes significant damage awards for its violation thereby changing the market for intrusively gathered information in an effort to reduce the occurrence of privacy invasion. Finally although the statute does not explicitly address social norms it may reflect an effort to use the law to reinforce social aspirations for greater privacy protections. [41]

One of the best protectors of privacy traditionally has been physical space: the torts of intrusion and trespass would protect a person's reasonable expectation of privacy if he secluded himself from the public. However, physical space as a protector of privacy and constraint on behavior is particularly subject to erosion by changed circumstances. For example, even though physical access to property may be limited, a photographer may attain the same proximity to her subject through the use of a telephoto lens. Therefore, for the physical space constraint to protect the subject's privacy against this non-physical intrusion, some additional restraint must prevent the photographer from using the telephoto lens: the absence of such technology; the cost of such technology; the moral sense that this technology should not be used for spying; or a law prohibiting such technology. Alternatively, the protection provided by the

---

41. *Ibid,* at 1378.

original constraint – physical space - could be translated, such that its protection is defined both in terms of property rights (to prevent physical intrusions) and in terms of "access rights" (to prevent non-physical intrusions). The California statute adopts this last option. In an effort to restore the privacy protection that physical barriers traditionally provided, the California statute makes tortuous the capturing of visual or audio images through the use of sensory-enhancing technology if these images could not have been captured without a trespass and without the enhanced technology. With this formulation, the tort expands the protection provided by physical space. Not only does the tort prevent people from walking into the physical space around a person's property; it also prevents them from using technology to "shrink" that space and thereby to "trespass" by non-physical means. The tort thus gives the physical space a new meaning that cannot be eroded by technological advances and reinforces the protection that space provides with a more permanent form of constraint. [42]

In addition to regulating physical space as a way of regulating privacy, the new California statute attempts to enhance privacy by regulating market for intrusively obtained information. The statute provides for damages that are more certain, and possibly greater than, those imposed by the common law intrusion tort. The damages provision consequently acts to increase the expected cost, and therefore to reduce the occurrence, of intrusive newsgathering. [43] In sum, perhaps the intended effect of the statute was to reflect and reinforce social norms that favour privacy.

---

42. *Ibid*, at 1378-79.

43. *Ibid*, at 1380.

In India, a leading case dealing with the question of publication and the right to privacy was *R. Rajagopal vs. State of Tamil Nadu,* [44] popularly known as "*Auto Shankar Case*". In this case the Supreme Court of India has expressly held that the "right to privacy", or the right to be let alone is guaranteed by Article 21 of the Constitution. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right of the person concerned and would be liable in an action for damages. However, position may be different if he voluntarily puts into controversy or voluntarily invites or raises a controversy. [45]

This rule is subject to an exception that if any publication of such matters are based on public records including court it will be unobjectionable. If a matter becomes a matter of public record the right to privacy no longer exists and it becomes a legitimate subject for comment by press and media among others. Again, an exception must be carved out of this rule in the interests of decency under Article 19(2) in the following cases, viz., a female who is the victim of a sexual assault, kidnapping, abduction or a like offence should not further be subjected to the indignity of her name and the incident being published in press or media. [46]

The second exception is that the right to privacy or the remedy of action for damage is simply not available to public officials as long as the

---

44. AIR 1995 SC 264.

45. *Ibid,* at 276.

46. *Ibid,* at 276. 48. *Ibid,* at 277.

criticism concerns the discharge of their public duties, not even when the publication is based on untrue facts and statements unless the official can establish that the statement had been made with reckless disregard of truth. All that the alleged contemner needs to do is to prove that he has written after reasonable verification of facts. The Court, however, held that the judiciary with its contempt powers and the legislature with its privileges stands on different footing. [47]

In this case the editor and the associate editor of the Tamil Magazine "Nakheeran" published from Madras moved the Supreme Court and asked for a writ restraining government officials from interfering with their right to publish the autobiography of Auto Shanker who had been convicted for several murders and awarded capital punishment. Auto Shanker had written his autobiography in jail which depicted close relationship between the prisoner and several IAS, IPS and other officials, some of whom were partners in several crimes. The announcement by the Magazine that very soon a sensational life history of Auto Shanker would be published created panic among several police officials that they might be exposed. They forced him by applying third degree method to write a letter addressed to the Inspector General of Prisons that he had not written any such book and it should not be published. The I.G. wrote to the publisher that it was false and should not be published.

It is to be noted that the petitioners did not show that they were authorized to publish the book. The question for consideration was whether a citizen could prevent another from writing his autobiography. Secondly, does an authorized piece of writing infringe the citizen's right

---

47. *Ibid,* at 277.

to privacy. Does the press have the right to an unauthorized account of a citizen's life. Thirdly, whether the Government could maintain an action for defamation or put restraint on press not to publish such materials against their officials or whether the officials themselves had the right to do so. The Court held that the state or its officials have no authority in law to impose prior restraint on publication of defamatory matter. The public officials can take action only after the publication of it is found to be false. Thus the editor or the publisher of the magazine have a right to publish what they allege to be the life story or autobiography of condemned prisoner in so far as it appears from the public records even without his consent or authorization. But if they go beyond that and publish his life-story, they may be invading his right to privacy and will be liable for the consequences in accordance with law. [48]

48. *Ibid*, at 277.

D. Computers

The human memory has been reinforced for thousands of years by writing, and over the last 100 years by typing and mimeographing. The invention of the computer has facilitated the storage and handling of information to a degree that can fairly be called revolutionary. The amount of information that can be accumulated is no longer limited by the storage space needed for masses of sheets of paper and metal cabinets, nor by the labour and wages of clerks and typists. The Bible, for instance, can be reproduced on a thin sheet of plastic less than two inches square. It is therefore feasible to include far more items than in the past. Also, computerized records are more durable than pieces of paper, and there is no incentive to get rid of them after a limited period of time. With regard to records concerning individuals, the scope for the invasion of privacy is greatly enlarged.[1] It is now technically feasible for all the information about individuals (medical, financial and so forth) to be brought together in one large data-bank. Obviously, this would wipe out one of the basic safeguards of privacy: that information should be seen only by those to whom it was given for their specific purpose – health details to the doctor or hospital, details of earning to the tax inspector etc.[2] Thus a significant threat to privacy posed by the advent of the computer lies in the so called 'data-banks'. These should be thought of not so much as computers, but as immense storage systems in which an astronomic amount of information can be permanently held and extracted in any sequence, and in any selected permutations, at any time. The usefulness of such systems to the

---

1. Mervyn Jones (compiled and edited), *Privacy*, 1971, at 52.

2. *Ibid*, at 60.

community is obvious, particularly in the fields of medical statistics, planning, simulation of economic models, prediction of demographic and other trends, and so forth. So long as the use of the data stored in the facility is confined to statistical purposes of this kind, the benefit is obvious. The danger arises only because, by the very nature of the facility, it provides an open invitation for the extraction of the full record of named individuals, legitimately by those who have official access to the facility, and possibly illegitimately by those who can obtain access by fraud, stealth or corruption. [3]

From the privacy point of view, the most alarming fact about the computer is the ease with which information can be elicited from it. Professor Westin writes: "Standardization of computer languages and the perfection of machines that translate one machine language system into another have made it possible for computers to communicate directly with one another so that data can flow in and out of separate 'systems'. To get information from computer, one needs to have either (a) another computer; or (b) a computer terminal, which is a much cheaper proposition; or (c) an ordinary telephone. [4]

In Britain, both computer-users (in general) and computer manufactures have shown themselves aware of the problem of privacy and willing to accept safeguards. The Conference called by the National Council of Civil Liberties and reported in the book *Privacy, Computers and You* [5], was willingly attended by representatives of the computer

---

3. Privacy and the Law, A report by Justice (1970)

4. *See*, *Ibid*, note 1 at 62.

5. B. C. Rowe (ed), *Privacy, Computer and You* (National Computing Center, 1972)

industry. Certain safeguards for privacy were found perfectly feasible.As the information enters the file, its origin, degree of confidentiality and destination within the file can be logged. Within the computer it is possible to hold all or parts of the information in sealed compartments, and to scramble it within these compartments. As it leaves the computer the content, time and name of the user can be logged. A system operating like the passkeys to a vault permits the imposing of any rules and safeguards an organisation may wish. Facilities for implementing these safeguards are now included in the various program packages offered by computer manufacturers. The way they are implemented is the private concern of the user, but the facility is there. We have yet to devise a code that cannot be broken, and it is true that, even if it is harder to gain access to computer files, the concentration of information within them could make it more worthwhile to try. But the facts to remember are these:
First, computerized information is held in a form that restricts access to those who are acquainted intimately both with computer systems in general and the system in question. Next, the imposition of monitoring and passkey techniques means that any betrayal of security needs the connivance of as many executives as one cares to nominate. Thirdly, the 'passkeys' can be changed more frequently than any physical key. And, finally, the logging of entries and withdrawals of information is automatic. The combination of connivance and technical skills needed to break into data banks is therefore considerably greater than those needed for entering ordinary filing systems. [6]

The Younger Committee also tackled this problem and

---

6. *Ibid.*

recommended built-in safeguards to prevent easy access to computerized information and undesirable disclosure: The fear of many of those outside the computer world who have given evidence relates mainly to access from terminals. In this connection it is important to bear in mind that links with terminals may be by private or public telephone lines or short wave radio. Access from terminals can be controlled by simply locking the terminal or the room containing it; by restricting access to sensitive information in the main computer store to specified terminals; by providing terminal-users with individual identity codes (such as keys, badges or tokens inserted at the terminal) or passwords which must accompany a request for information, by requiring an authorized terminal-user to answer random questions about his background to which only he will know the answers; or by voice identification techniques (still at an early stage of development). [7]

Devices of this kind, however, are very far from allaying all the anxieties which arise from the increasingly widespread use of the computer. It must be borne in mind that computer technology is already a massive industry employing thousands of people who are recruiting at high speed and without any great degree of discrimination. They are rapidly trained; there is no long standing tradition of discretion and responsibility, comparable, for instance, to the traditions of the medical profession. In the nature of things, it seems inevitable that some among the many thousands of computer employees will be indifferent to considerations of privacy; some will regard safeguards of confidentiality as a mere nuisance involving extra work, to be ignored whenever it is safe; and a few will be open to bribes and inducements, or willing to make

---

7. *Report of the Committee on Privacy* (Cmnd.5012) (London : HMSO,1972).

unauthorized disclosures because they see this as a trivial matter. The atmosphere of computer work accentuates the dangers; the stress is placed on speed and convenience, and the highest value is placed on meeting the requirements of customers and providing a 'full-service' [8].

The Younger Committee came up with a series of remedies which amounted to a kind of privacy charter:

> There could be an incentive to cover the cost of the acquisition and recording of information by using it for purposes additional to that for which it was originally collected. For example a computerized record of subscribers to a trade publication might well prove useful to the manufacturers of certain products advertised therein. The situation could be a clear breach of privacy in so far as it could be held that private information (a name and address) given solely for the purpose of receiving a magazine is passed on without the authority of the originator.
>
> Therefore :
>
> (1) Information should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes; and
>
> (2) Access to information should be confined to those authorized to have it for the purpose for which it was supplied.

Furthermore, because it is often cheaper to collect all available information in one operation and because computers have

---

8. *See, Ibid,* note 1 at 78.

the capacity to store it, there could be a double incentive for the owners of computers to hoard large amounts of information some of which, though not essential now, might prove useful at some later date. We believe that:

(3) The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose.

A great deal of personal information is acquired to provide statistics to assist planning and other research, or is acquired for some other purpose and subsequently adapted to a form suitable for such ends. Planners and researchers, however rarely need to know identities of individuals. Therefore:

(4) In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.

Every system should be so designed that in situations where printout is appropriate an individual can on request be told of the contents of the record. Therefore:

(5) There should be arrangements whereby the subject could be told about the information held concerning him.

We are not convinced that considerations of privacy are at present sufficiently in the minds of computer users and we think that more regard should be paid to such considerations than is the case now. Therefore:

(6) The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.

A security system would be incomplete however, if it did not include provision for the detection of an irregularity. Therefore:

(7) A monitoring system should be provided to facilitate the detection of any violation of the security system.

Computers have the capacity to retain information in effect indefinitely so that it is occasionally stored, in the form of discs or tapes, with little regard to a time limit. Therefore:

(8) In the design of information systems, period should be specified beyond which the information should not be retained.

(9) Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.

(10) Care should be taken in coding value judgments. [9]

Nevertheless, the Committee was forced to conclude that no safeguards can provide against all conceivable eventualities. Lapses are bound to occur, simply because this field of technology is new, experimental and constantly developing; and also because the safeguarding of privacy has never been a major consideration.

---

9. *See, Ibid*, note 7.

Data Protection and privacy.

Since the Warren and Brandeis definition of privacy as the 'right to be let alone' a great amount of time has been devoted to defining an exhaustive list of the constituent components of the term 'privacy'. However, what does seem to be agreed upon is the extent to which the meaning of 'privacy' is dependant on a nation's culture. The 1978 Lindop Report on data protection differentiated between the principles upon which data protection legislation is based and justified and those that lie behind the 'right to privacy'. It stated:

> (T)he function of a data protection law should be different from that of a law on privacy: rather than establishing rights, it should provide a framework for finding a balance between the interests of the individual, the data user and the community at large [10].

Such a balancing act can be easily recognised in the two motives behind the Council of Europe Convention which are : the threat to individual privacy posed by computerization ; and the need to maintain a free flow of information in an international market. The Convention therefore attempts to reconcile Article 8 of the European Human Rights Convention, concerning an individual's right to privacy, with the principle of free flow of information enshrined in Article 10 of the Human Rights Convention [11].

Despite this difference between the concept of data protection and privacy, developing data protection case law can extend the scope of the legislation to wider questions regarding an individual's 'right to privacy' In Germany, a Constitutional Court decision declared unconstitutional an Act which had authorized the governmentt to undertake a comprehensive

---

10. Chris Reed, (ed), *Computer Law,* 3rd Edition, 1st Indian Reprint (2000), 329.

11. *Ibid,* at 328.

population census. The Court declared that each data subject has a right to determine in general the release and use of his or her personal data; thus establishing a constitutional right of individual 'informational self-determination'. The decision also led to a fundamental review of the German Data Protection Act. It has also been noted that some judicial opinion within the European Court of Human Rights has begun to use the Council of Europe Convention on Data Protection to enliven and strengthen Article 8 of the European Convention on Human Rights. [12]

A related question concerns the relationship between data protection legislation and freedom of information laws. Access rights to public archives, for example, could lead to infringements of an individual's privacy. In Quebec, Canada, legislation has been adopted covering both access to documents held by public bodies and the protection of personal information in the same statute. Conversely, in the UK, it has been claimed that the Data Protection Act, 1984 has been used as an excuse by some government authorities to refuse the disclosure of legitimate public documents, and therefore maintain greater secrecy. [13]

In order to prevent organisations from avoiding data protection controls, and therefore guaranteeing a free flow of information, international governmental organisations have become involved in attempting to obtain international harmonisation for data protection legislation. These include the Council of Europe, the OECD, the United Nations and the European Community.

---

12. Ibid, at 329-30.

13. Ibid, at 330.

The Council of Europe

The Council of Europe has been the major international force in the field of data protection since the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was agreed upon. A majority of the 39 Council of Europe members have signed the Convention, and have therefore accepted an obligation to incorporate certain data protection principles into national laws. The Convention came into force on 1 October 1985 when five countries had ratified it : Sweden, Norway, France, Federal Republic of Germany and Spain. The Council of Europe has been involved in this area since 1968, when the Parliamentary Assembly passed recommendation 509(68) asking the Council of Ministers to look at the European Human Rights Convention to see if domestic laws gave adequate protection for personal privacy in the light of modern scientific and technological developments. The Council of Ministers asked the Committee of Experts on Human Rights to study the issue and they reported that insufficient protection existed.

A specialist Committee of Experts on the Protection of Privacy was subsequently asked to draft appropriate resolutions for the Committee of Ministers to adopt. In 1976 the Committee of Experts on Data Protection was established. Its primary task was to prepare a convention on the protection of privacy in relation to data processing abroad and trans-frontier data processing. The text of this convention was finalised in April, 1980, and opened for signature on 28 January, 1981. The convention is based on a number of basic principles of data protection, upon which each country is expected to draft appropriate legislation. Such legislative provisions will provide for a minimum degree of harmonisation

between signatories, and should therefore prevent restrictions on trans-border data flows for reasons of 'privacy' protection.

Since 1981 the Committee of Experts on Data Protection has been primarily involved in the drafting of sectoral rules on data protection. These form part of an ongoing series of recommendations issued by the Committee of Ministers designed to supplement the provisions of the Convention. There are currently Council of Europe working parties looking into the media sectors; and the data protection issue created by the use of personal identification numbers and genetic data. No enforcement machinery was created under the Convention, and therefore any disputes have to be resolved at the diplomatic level. [14]

Organisation for Economic Cooperation and Development

The Organisation for Economic Cooperation and Development was established in 1961 and currently comprises 28 of the leading industrial nations. The nature of organisation has meant that interest in data protection has centred primarily on the promotion of trade and economic advancement of member states rather than 'privacy' concerns.

In 1963 a Computer Utilization Group was set up by the 3rd Ministerial meeting. Aspects of the group's work concerned with privacy went to a subgroup, the Data Bank Panel. This body issued a set of principles in 1977. In the same year the Working Party on Information Computers and Communications Policy (ICCP) was created out of the Computer Utilization and Scientific and Technical Policy Groups. Within this body the Data Bank Panel became the Group of Government Experts

---

14. Ibid, at 330-31

on Trans-border Data Barriers and the Protection of Privacy. Its remit was:

> To develop guidelines on basic rules governing the trans-border flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation.

The OECD guidelines were drafted by 1979, adopted in September 1980, and endorsed by the UK Government in 1981. The guidelines are based, as is the Council of Europe Convention, upon eight self-explanatory principles of good data protection practice. The Republic of Ireland became the last country to sign the guidelines in January, 1987. the guidelines are simply a recommendation to countries to adopt good data protection practices in order to prevent unnecessary restrictions on trans-border data flows and have no formal authority. However, some companies and trade associations, particularly in the US and Canada, have formally supported the guidelines. [15]

The United Nations

The United Nations has only focused on the human rights aspects of the use of computer technology comparatively recently. In 1989 the General Assembly of the Commission on Human Rights adopted a set of draft guidelines for the regulation of computerised personal data files. These draft guidelines were subsequently referred to the Commission on Human Rights' special rapporteur, Mr. Louis Joinet for redrafting, based on the comments and suggestions received from member governments and other interested international organisations. A revised version of the guidelines

---

15. Ibid, at 332

was presented and adopted in 1990.

The guidelines are divided into two sections. The first section covers principles concerning the minimum guarantees that should be provided in national legislations. These 'principles' echo those put forward by both the Council of Europe Convention and the OECD guidelines except for three additional terms:

a) Principle of non-discrimination - sensitive data, such as racial or ethnic origin, should not be compiled at all.

b) Power to make exceptions – justified only for reasons of national security, public order, public health or morality.

c) Supervision and sanctions – the data protection authority shall offer guarantees of impartiality, independence vis-`a-vis persons or agencies responsible for processing and technical competence.

The second section considers the application of the guidelines to personal data files kept by governmental international organisations. This requires that international organisations designate a particular supervisory authority to oversee their compliance. In addition, it includes a 'humanitarian clause' which states that:

> A derogation from these principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance.

Such a clause is intended to cover such organisations as Amnesty International, which holds large amounts of personal data but would be wary of sending information out to a data subject on the basis of an access request made while the person was still imprisoned. [16]

---

16. Ibid, at 332-33

The European Community

Despite interest and involvement in data protection and privacy issues for nearly two decades from both the European Parliament and the Commission, the emergence of a Directive concerning this area only appeared in 1990.

The European Parliament's involvement in data protection issues has primarily been through its Legal Affairs Committee; though the issue has been subject to parliamentary questions and debates for the past 10 years. In 1976, the European Parliament adopted a resolution calling for a Directive to ensure that community citizens enjoy maximum protection against abuses or families of data processing as well to avoid development of conflicting legislation.

In 1977 the Legal Affairs Committee established the Subcommittee on Data Processing and the Rights of the Individual. It produced the 'Bayerl Report' in May 1979. The resultant debate in the European Parliament led to recommendations being made to the Commission and the Council of Ministers concerning the principles that should form the basis of the Community's attitude to data protection. These recommendations called on the European Commission to draft a Directive to complement a common communications system, to harmonise the data protection laws and to secure the privacy of information of individuals in computer files.

A second Parliamentary report, the 'Sieglerschidt' Report, was published in 1982. The report noted that data transmission in general should be placed on a legal footing and not be determined merely by technical reasons. It recommended the establishment of a "European Zone" of members in the EEC and Council of Europe, within which authorization prior to the export of data would not be needed. It also

indicated that initiatives such as a Directive were still necessary. Following the report, a resolution was adopted by the European Parliament on 9th March, 1982 calling for a Directive if the Convention proved inadequate. In July 1990 the European Commission finally published a proposed Directive on data protection. After considerable controversy and political debate at all stages of the legislative process, the general framework Directive on data protection was finally adopted by the European Parliament and Council on 24th October, 1995. The Commission also expressed its desire to protect the rights of individual data subjects and in particular their right to privacy (Article 1(1)). [17]

The United Kingdom Data Protection Act, 1984.

In 1961 Lord Mancroft introduced a Right of Privacy Bill which finally led to the passage of the Data Protection Act, 1984. This first private member's Bill was followed by four others, from both the House of Commons and the Lords, until the Government decided to establish a formal committee of inquiry into this area, precipitated by a parliamentary debate on a private members Bill. In May 1970 a Committee on Privacy was appointed under the chairmanship of Kenneth Younger. Its terms of reference were:

> "To consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons and organisations, or by companies, and to make recommendations."

---

17. *Ibid,* at 333-35

The Committee's purview was limited to the private sector. The final report was presented to Parliament in July 1972.[18] During its establishment the Committee set up a special working party on computers. Its terms of reference were :

> "To examine the alternative means of controlling the handling of information by computers and to recommend those which seem most appropriate having regard to practicability and cost, and also to survey the present scale of computer use and likely evolution, with special reference to the implications for controls."

The working party concluded that: put quite simply, the computer problem as it affects privacy in Great Britain is one of the apprehensions and fears and not so far one of facts and figures.[19] The Committee noted that the main areas of public concern were with universities, bank records and credit agencies. It recommended that an independent body (standing commission) composed of computer experts and lay persons, should be established to monitor growth in the processing of personal information by computer, as well as the use of new technologies and practices.

In response to the Younger Report, a white paper, *Computers and Privacy* (Cmnd 6353), was presented to Parliament by the Home Secretary, Roy Jenkins, in December 1975. In it the Government accepted the need for legislation to protect computer based information. Despite the concerns expressed in the Younger Report with regard to manual records, the Government felt that computers posed a special threat to individual privacy:

The speed of computers, their capacity to store, combine, retrieve

---

18. *Report on the Committee on Privacy* (Cmnd. 5012) (London: HMSO, 1972)

19. *Ibid,* at 179.

and transfer data, their flexibility and the low unit cost of the work which they can do have the following practical implications for privacy: (1) they facilitate the maintenance of extensive record systems and the retention of data on those systems; (2) they can make data easily and quickly accessible from many distant points; (3) they make it possible for data to be transferred quickly from one information system to another; (4) they make it possible for data to be combined in ways which might not otherwise be practicable; (5) because the data are stored , processed and often transmitted in a from which is not directly intelligible, few people may know what is in the records, or what is happening to them.

The Government. also issued a second White Paper entitled *Computers: Safeguards for Privacy* (Cmnd 6354) which agreed with the comments made by the Younger Report with regard to the concerns generated by public sector information. The paper considered the extent, nature and proper safeguarding of personal data held on computers in the public sector. The White Paper proposed legislation to cover both public and private sector information systems. The creation of a Data Protection Authority was also proposed, to supervise the legislation and ensure that appropriate safeguards for individual privacy were implemented. In order to provide a detailed structure for the proposed Data Protection Authority the government established a Data Protection Committee, a twelve-person committee, under the chairmanship of Sir Norman Lindop, which reported in 1978. [20]

---

20. *See, Ibid,* note 10, 338-39.

The Lindop Report proposed that a number of data protection principles should form the core of the legislation with the Data Protection Authority being responsible for ensuring compliance with those principles. In particular, the Authority would be required to draft codes of practice for various sectors based on consultations with interested parties and associations, which would then become law as statutory instruments. Failure to comply with a code would lead to criminal sanctions. Overall the Lindop Report was concerned to produce a flexible solution which would not act so as to hold back the growing use of computers within both the public and private sector. After the fall of the government in 1979, legislation on data protection was delayed. Finally in 1982 the government issued a White Paper entitled *Data Protection: the Government's Proposal for Legislation* (Cmnd 8539). In the White Paper the idea of a Data Protection Authority was replaced by an individual Registrar of Data Protection. The Data Protection Act, 1984, received the royal assent on 12th July, 1984. The provisions of the Act were phased over a three-year period, with the Act becoming fully operational on 11th November, 1987. The Act was limited to computer data because the government felt that computers posed a unique threat to individual privacy through their ability to store, link and manipulate large amounts of data. [21]

Digital technology and new communication systems have made dramatic changes in our lives. Business transactions are being made with the help of computers. Business community as well as individuals are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form is cheaper. It is easier to store, retrieve and

---

21. *Ibid*, at 340.

speedier to communicate. People are aware of these advantages but they are reluctant to conduct business or conclude transactions in the electronic form due to lack of legal framework. At present many legal provisions recognize paper based records and documents which should bear signatures. Since electronic commerce eliminates the need for paper based transactions, therefore, to facilitate e-commerce, there was a need for legal changes. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996. India being signatory to it had to revise its laws as per the said Model Law. Keeping in view the above, the Information Technology Act, 2000 was passed by Indian Parliament. [22]

Just like the development of any new area such as a new geographical territory or a new financial instrument or a new invention, the internet is a new area where there are a majority of beneficial users, as well as, a few who like to exploit the others. The Information Technology Act, 2000 performs the dual role of encouraging digital interaction, as well as, booking the 'net criminals'. The Act provides for a legal framework so that information is not denied legal effects, validity or enforceability solely on the ground that it is in electronic form. This is done by legally recognizing electronic records [23] and electronic signatures [24] in government and its agencies, as well as, their use by

---

22. Nandan Kamath, *Guide to Information Technology Act, 2000* (2000 edn). 3.

23. "Electronic Record" mean data, record or data generated, image or sound received or sent in an electronic form or microfilm or computer generated microfiche. *See,* Sec 2 (f) and Sec 4.

24. "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Sec 3 of the Act. *See,* Sec 2 (p) and Sec 5.

private individuals. Any subscriber may authenticate an electronic record by affixing his digital signature which shall be affected by the use of Asymmetric Crypto System and Hash function which envelop and transform the initial electronic record into another electronic record. Any person by the use of public key [25] of the subscriber can verify the electronic record. The private key [26] and the public key are unique to the subscriber and constitute a functioning key pair. [27] A public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. For commerce on the internet, it is necessary to provide a way to send keys to wide variety of persons, many of whom are not known to the sender, where no relationship of trust has developed between the parties. This is where the Certifying Authorities have a role to play. A Certifying Authority is entrusted with the function of identifying persons applying for signature key certificates, verify their legal capacity, confirm the attribution of a public signature key to an identified physical person by means of a signature key certificate, maintain on-line access to the signature key certificates with the agreement of the signature key owner and take measures so that the confidentiality of a private signature key is guaranteed. The Act further provides that if any person publishes a Digital Signature Certificate or otherwise makes it available to any person with the knowledge that (i) the Certifying Authority listed in the certificate has not issued it; or (ii) the subscriber listed in the certificate has not accepted it; (iii) the certificate has been revoked or suspended unless

---

25. "Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate [Sec 2 (zd)]

26. "Private Key" means the key of a key pair used to create a digital signature. [Sec 2 (zc)]

27. Sec 3.

such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation, he shall be punished with imprisonment upto two years or with fine upto one lakh rupees, or with both.[28] Prior to the aforesaid Act in India and similar such enactments all over the world such actions were difficult to book the hackers [29] due to the definition of 'unlawful entry'. The definition was mostly restricted to physical actions. Since the hacker did not physically break into the office or house of the victim, such persons in the initial years were not convicted. [30]

Computer Network Break-ins

Using software tools installed on a computer in a remote location, hackers can break into computer systems to steal data, plant viruses or Trojan horses, or work mischief of a less serious sort by changing user names or passwords. Network intrusions have been made illegal under the Information Technology Act, 2000, but detection and enforcement are still difficult.

Section 43 is the basic section covering computer break-ins. It states that if any person without permission of the owner or any other person who is in charge of a computer, computer system or computer

---

28. Sec 73.

29. Hacker is a term used to define a person who does not possess any authority to gain access to a particular computer but does so by trying different passwords on his own. This either on a trial or error basis or under a specially written software or by intercepting the password (stealing) when used by the authorized user.

30. Nitant P. Trilokekar, *A Practical Guide to Information Technology Act,* November 2000, Millennium Edn. at 51-52

network;

(a) Accesses or secures access to such computer, computer system or computer network;

(b) Downloads, copies or extracts any data, computer database, or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium ;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer etc.;

(d) Damages or causes to be damaged any computer, etc., data, computer database or any other programmes residing in such computer etc.;

(e) Disrupts or causes disruption of any computer etc.;

(f) Denies or causes the denial of access to any person authorized to access any computer, etc. by any means;

(g) Provides any assistance to any person to facilitate access to a computer, etc., in contravention of the provisions of the Act, rules or regulations made thereunder;

(h) Charges the services availed of by any person to the account of another person by tampering with or manipulating any computer etc;

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

One more sanction under which prosecution could be made is under Section 66 where 'hacking' is defined and punishment is also specified. [31]

---

31. Sec 66 (1): whoever with the 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 alters any information residing

Industrial Espionage

When any computer is attached to the internet, an unlawful entry can be made by any person in the reverse direction into the computer and thus to any data in it as well into the computers attached to this computer. A hacker can get virtual free hand including viewing of tenders, purchase prices and even inter-office memos. Corporations, like governments, love to spy on the enemy. Networked systems provide new opportunities for this, as hackers-for-hire retrieve information about product development and marketing strategies, rarely leaving behind any evidence of the theft. The difficulty of prosecution here is that the victim has himself visited the site voluntarily and downloaded the software voluntarily. In such a case, there is no effort on the part of the accused of trying to break in the computer resource like that of the hackers. Again the relevant section under the Indian Act is Section 43. Though the perpetrator has not hacked into the system, in such cases he has definitely secured access without permission of the victim at least for that part of the program that searches and retransmits information from his computer. [32]

Copyright Piracy

This is the easiest known abuse of the internet. We have available at the click of a mouse, thousands of written works from all over the world. If some of it is downloaded and the name of the author substituted, the

---

in a computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking.

Sec 66 (2):Whoever commits hacking shall be punished with imprisonment upto three years or with fine which may extend upto two lakh rupees or with both.

32. *Ibid*, at 54-55

piracy is committed. Apart from written words, even works of art (drawings / photos) can be easily downloaded. If a person later sells it claiming the work to be his, the copyright infringement is committed. This is a crime that is not easy to police. Copyright problems are the bane of the music industry. Since the piracy is done in a digital format, the end result is sharp and clear enough even for the discerning music lover. The only thing preventing a music lover from downloading a pirated song is his own righteous behaviour and not the quality of the song. The only option left for policing is to remain alert and try to track the sites as the offers are made. But due to the frequent change in site address, the customers will be troubled and eventually not make efforts to locate the relocated site. This way, if the demand dies down, the lack of demand will force out such sites. In this type of crime, typically a published article is used or a CD is taken and digital conversion is uploaded on the internet. The Information Technology Act, 2000 does not specifically cover such crimes. Only the Copyright and Patents Act can cover such cases. [33]

Software Piracy

According to estimates by the US Software Publisher's Association, as much as $7.5 billion of American software may be illegally copied and distributed annually worldwide. These copies work as well as the originals, and sell for significantly less money. Piracy is relatively easy, and only the largest rings of distributors are usually caught. The Information Technology Act, 2000 does not cover such crimes too and only the Copyright and Patents Act can cover such cases. [34]

---

33. *Ibid*, at 55-56

34. *Ibid*, at 56

Child Pornography

This is a crime in which images of children in varying stages of dress and performing a variety of sexual acts are acquired. Legally speaking, people who use or provide access to child porn face the same charges whether the images are digital or on a piece of photographic paper. The Information Technology Act, 2000 does not give child pornography any special status. Section 67 may be mentioned in this regard: Section 67 of the Act reads: "Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effects is such as to tend to deprave and corrupt persons who are likely; having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two tears and with fine which may extend to twenty five thousand rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to fifty thousand rupees."

Mail Bombings

By instructing a computer to repeatedly send electronic mail (E-mail) to a specified person's E-mail address, the cyber-criminal can overwhelm the recipient's personal account and potentially shut down entire systems. The Information Technology Act, 2000 does not specifically cover such crimes. It is dealt with in the Copyright and Patents Act. [35]

---

35. *Ibid*, at 57-58

Password Sniffers

Password sniffers are programs that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can then impersonate an authorized user and log in to access restricted documents. Under the Information Technology Act, 2000, in the actual act of sniffing, the sniffers are not invading any computer systems. When the sniffer has used the collected password to take free access to a system, the crime gets covered by the Act under Sections 43(a) and 43(g). [36]

Spoofing

Spoofing is the act of humbugging by disguising one computer to electronically "look" like another computer in order to gain access to a system that would normally be restricted. There is no unauthorized entry but merely the identity is duplicated so that the traffic of the data is diverted to the wrong computer. The Information Technology Act, 2000 does not specifically cover such crimes. The Indian Penal Code can be used to initiate proceedings of fraud. [37]

Credit Card Fraud

The US Secret Service believes that half a billion dollars may be lost annually by consumers who have credit card and calling card numbers stolen from on-line databases. Security measures are improving and traditional methods of law enforcement system seem to be sufficient for prosecuting the thieves of such information. The Information Technology

---

36. *Ibid*, at 58

37. *Ibid*, at 59.

Act, 2000 does not specifically cover such crimes. Sniffers are the ones who gain access to credit card numbers. These are used on the internet with the other 'identification' information which was gained in the same manner. Signatures are not forged since signatures are not used. [38]

Cyber Squatting

Cyber squatters usually grab a well known trademark which they register as domain name for ulterior purposes. They try and sell this domain name back to the rightful owners for a fancy price. This is done to mislead the internet users to believe that they are rightful owners of the brand. The Act does not specifically cover such crimes. [39]

Misleading Search Words

Some of the search results throw up absolutely unrelated sites. This is more by deliberate action than by accident. The idea is to grab a viewer who may be either an undecided viewer or searching for a competing site. The Act does not specifically cover such crimes. [40]

It may be noted that Section 72 of the Act specifically provides for remedy for breach of confidentiality and privacy. Section 72 states that if any person has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and discloses the same to any other person, he shall be punished with imprisonment up to two years, or with fine up to one lakh rupees, or with both.

---

38. *Ibid*, at 59-60

39. Ibid, at 60.

40. *Ibid*, at 60-61.