Chapter Five

Judicial Response to Right to Privacy

5.1 Introduction
5.2. Judicial decisions on Right to Privacy and Data Protection in India
5.2.1 Before Independence
5.2.2 After Independence
5.2.2.1 Right to property-search and seizure
5.2.2.2 Right to personal liberty
5.2.2.3 Right to privacy of communication
5.2.2.4 Right to disclosure of information
5.2.2.5 Right to Privacy under Information Technology Act, 2000
5.2.2.6 Right to Privacy as a Fundamental Right
5.2.2.7 Right to Protection of data under Indian Law
5.2.2.8 Right to be Forgotten
5.2.2.9 Discussion
5.3 Judicial decisions on Right to Privacy and Data protection in other countries
5.4 United States of America
5.4.1 Right to Search and Seizure
5.4.2 Right to Personal liberty
5.4.3 Right to Privacy of Personal communication
5.4.4 Right to Disclosure of Information
5.4.5 Right to Protection of Data
5.4.6 Discussion
5.5. United Kingdom
5.5.1 Right to Search and Seizure
5.5.2 Right against Breach of Confidence
5.5.3 Photographs and Right to Privacy
5.5.4 Right to Protection of Data
5.5.5 Discussion
5.6 European Union
5.6.1 Right to Protection of Data
5.6.1.1 Freedom of Movement of Data on Internet
5.6.1.2 Health Data and Right to Privacy
5.6.1.3 Cross Border Data Transfer and Right to Privacy
5.6.2 Photographs and Right to Privacy
5.6.3 Right to be Forgotten
5.6.4 Discussion
5.7 Judicial Trends in Right to Privacy: Comparative Analysis

5.1 Introduction

Use of computer, internet and information technology facilitate the personal and business transactions at person's own convenience. For use of technology, submitting personal information is a precondition. By each access, the personal information is deposited and gathered in large quantity with the entity which provides service. It is expected that this information shall remain confidential and private. Threat to personal information has increased due to globalisation and privacy of person is endangered. This threat is not limited to physical harm due to cyber-crimes but affecting the liberty and freedom to make choices due to excessive marketing. Even the information collected by government for provision of services, privacy and confidentiality of it may also be threatened.

By enacting different legislations, legal systems tried to control and regulate transactions done using information technology. The major challenge before any legal system is to balance the rights of the persons and interests of the state. In India after 1990, due to globalisation, use of computers and internet had increased. To protect the business interests, and e-commerce transactions, The Information Technology Act, 2000 was enacted. To make it more strong, provisions controlling cyber-crimes were added after its amendment in 2008. But for the protection of the information which is deposited and gathered with the body corporates-entities which provide services- its control and regulation under it is inadequate.

In the days of absence of legislative control mechanism i.e. from the beginning of 20th Century, the protection to privacy was provided by courts. Courts have provided protection against the state actions threatening physical, proprietary privacy. They also provided protection against the informational privacy invaded by state as well as private entities as innovative uses of advanced technology harming it. This protection was granted by interpreting the existing laws including provisions for fundamental rights under Constitutional law.

Illustrating the Court's function while controlling the invasion, Supreme Court held in Canara Bank[1] that "Intrusion into privacy may be by a) legislative provisions, b) administrative/executive orders and c) judicial orders. The

[1] District Registrar and Collector, Hyderabad v. Canara Bank, (2005) 1 SCC 496

legislative intrusion must be tested on the basis of reasonableness as guaranteed by the Constitution and for that purpose court can verify the proportionality of intrusion i.e. the purpose sought to be achieved. Administrative or executive action is concerned, it is to be reasonable and this reasonableness is verified from facts and circumstances of the case. As for the judicial action, e.g. intrusion may be through issuance of warrant, the court must have sufficient reason to believe that the action is necessary to uphold state interest. For this extent of the action shall be prescribed which only protect the state interest and not encroach the rights of the person unnecessarily. The order of the Court must observe that the action will be taken in good faith, intended to preserve evidence, or intended to prevent sudden danger to person or property"[2].

The researcher has discussed the judicial decisions for the protection of Right to Privacy and data protection in different countries including India in the following paragraphs.

5.2 Judicial decisions on Right to Privacy and Data Protection in India

Though before independence, some decisions were given by the Supreme Court of undivided India, in which the Right to Privacy was upheld. In India, the vacuum of absence of common law provisions for protection of privacy is filled with the judicial activism of Supreme Court. The Supreme Court of India has come to rescue of common citizen by construing 'Right to Privacy' as a part of fundamental right to life and personal liberty under Art. 21 of Constitution of India.

As in other judicial systems, the right was associated with enjoyment of property in India, may it be house or land. As India was ruled by England, we can see the development from the 19th Century. The courts in British-India upheld the right in different cases. These decisions were given by British India Courts and the Judges of Sardar Diwani Adalats.

[2] District Registrar and Collector, Hyderabad v. Canara Bank, (2008) 1 SCC 496

5.2.1. Before Independence

The protection of right to privacy had appeared in the reports of British India courts for the first time after 1850. In 1855, in the decision of North-Western Province in Nuth Mull (1855)[3], the question of privacy arose. In this case Begbie, Smith and Jackson JJ held on appeal from the decree of the principal Sadr Amin of Delhi, that the erecting by the defendant of a new house, so that the plaintiff's premises were overlooked from the roof of the new house and their privacy thereby interfered with, gave the plaintiff a cause of action against the defendants.

Reports of some of the decisions are found in other decided cases after those cases. As this case of Nuth Mull was referred by Chief Justice Edge in **Gokal Prasad (1888)[4]**, where the court observed that due to destruction of records during mutiny of 1857, it is not possible to ascertain whether there was a custom of privacy in this part of India. It was never proved or called in question prior to 1855 and owing to same cause and to absence from the report of the case on Nuth Mull and Kureem Oolah Beg of information on the point it is not possible to ascertain whether the judges of Sadr Diwani Adalat of North-Western Provinces were following the law as it was found existing or decided the case from the facts found.

In the same way, in case of Gokal Prasad, C.J. Edge referred to a number of cases on privacy. They were, Gunga Prasad (1862)[5]**,** where Ross and Roberts, JJ. did not suggest any doubt that a right to privacy could exist, in Banaras case of Goor Das(1867)[6]-and also in Moradabad case of Ram Baksh (1867)[7], Morgan C.J. and Spankie J. expressly recognised the existence of a right to privacy. In 1886, Mata Prasad v. Behari Lal,[8] Straight and Mahmood JJ. evidently considered that the right to privacy could exist in respect of a house in the city of Allahabad.

[3] Nuth Mull v/s Zuka-Oolah Beg Sr.D.A.N.W.P.R.1855,
[4] Gokal Prasad v.Radho ILR Allahabad (10), 358 (1888),
[5] Gunga Prasad v. Salik Prasad S.D.A.N.W.P. Rep. 1862 Vol. II, 217
[6]Goor Das v. Manohar Das N.W.P.H.C. Rep. 1867, 269 cited in Gokal Prasad (1888) at www.indiakanoon.org/doc/103879 (Last visited on December 11, 2019)
[7] Ram Baksh v. Ram Sookh N.W.P.H.C. Rep. 1867, 269
[8] S.A. No.8 of 1856 (unreported)

Pro. Winfield[9] in 1931, had to fall back on Indian cases to persuade the House of Commons to extend the right of privacy to British nationals. But the right was not given by recognising right to privacy. This right was given by provisions of trespass and defamation. So the emphasis was only on proprietary rights. It was against the interests of the government to grant right to privacy in full as British were ruling the country. After independence Indian government was following the footsteps of British and right to privacy was not provided under Indian laws. While making the constitution, the constitutional committee also opposed to include this right in the Part III of the constitution as a fundamental right.

5.2.2. After Independence

Under Indian Constitution, there is no specific enactment for Right to Privacy as such and also there was no legislation for protection of privacy. Therefore the invasion on the right by was challenged on the ground of invasion on right to life and liberty i.e. Art. 21. Various contours of right to life and liberty including right to privacy are explored by the courts. Courts, in many cases touched the various aspects of right to privacy, i.e. against property for search and seizure to disclosure of information and upheld this right under the fundamental right governed under Article 21 i.e. Right to Life and several other provisions of the Constitution read with the Directive Principles of the State Policy. Some of the aspects of Right to Privacy which were given protection by the Supreme Court are discussed in following paragraphs.

1.2.2.1 Right to Search and Seizure

First notable expression of opinion on the 'Right to Privacy' with other issues of violation of fundamental right under Art. 20 (3) was in decision by Supreme Court in 1954. The power of state for search and seizure was thoroughly discussed and considered by Hon'ble Supreme Court in **M.P. Sharma (1954)**[10], where the allegation was that the company had emblazed the large sum of money and to defraud the shareholders falsified the accounts books. Offences were registered and search warrants were issued to search the documents concerning the property and records were seized. It was alleged that fundamental right of

[9] Percy H. Winfield, "Privacy" 47, L.Q.R. 29-30 (1931)
[10] M.P. Sharma v. Satish Chandra, District Magistrate, (1954) SCR 1077

the petitioner under Art. 19(1) (f) and Art. 20(3) are violated because of the searches. The reliance was also put that search and seizure has violated the right to privacy of the petitioner.

The Hon'ble Supreme Court had rejected the contention of violation of fundamental right under Art.19 (1) (f) but considered whether the searches was violating the fundamental right under Art. 20(3). The court observed that the searches were conducted according to the provisions of Criminal Procedure Code. Justice Jaganndhadas observed that searches and seizures do not infringe the fundamental right guaranteed by Art. 20 (3). It was held that if observed carefully, it is evident that search and seizure under Indian law is not termed compulsory. Both are different matters under the law. The notice to produce documents is issued to party concerned and his production is compliance therewith. Person is obliged to submit and therefore production is not testimonial act within the meaning of Art. 20 (3). But search warrant is issued to the police officer, a government servant, who is empowered to conduct the search. So both actions are directed to two different persons. The search and seizure both acts are performed by police officer and the person has to allow the police to conduct search and seizure. So such act of allowance is not testimonial act.[11] It was held that guarantee of self-incrimination is not offended by search and seizure.

The petitioner had relied on the contention that due to search and seizure, his right to privacy is violated and referred the case Boyd v. U.S., in which USA Supreme Court held that incriminating evidence obtained by illegal search and seizure violates the Fourth and Fifth Amendments of American Constitution which provide for right to privacy. Tracing the history of Indian legislation Supreme Court of India, observed that provisions of search and seizure are contained in Cr. P.C. and conducted after obtaining search warrant. It was held: "In any system of jurisprudence, an overriding power of state for protection of social security and that power is necessarily regulated by law. When the constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of fundamental right to privacy,

[11] M.P. Sharma v. Satish Chandra, District Magistrate, (1954) SCR 1077. P. 1096

analogous to the Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of stained construction. Nor is it legitimate to assume that the constitutional protection under Art. 20(3) would be defeated by the statutory provisions for searches".[12]

The protection was denied in other cases involving the search and seizure under Criminal Procedure Code. The Court denied that it infringes the fundamental right under Art. 20 (3). In **Pooranmal(1974)**[13], a search conducted by Income Tax Authorities under s. 132 of Income Tax Act and contention was raised that the search and seizure made by the authorities was illegal. Dismissing the petition, the Court held that the search and seizure are the powers regulated by Cr. P.C. and in this case the powers were exercised properly and therefore not illegal. It was observed by the Court that the evidence collected by illegal search cannot be excluded on ground that it is invasion of privacy because there is no specific fundamental right to privacy. This decision weakened the right of individual against the illegal search and seizure of the evidence. Moreover Right to Privacy was also derecognised.

This point of view of Supreme Court is also visible in **V.S. Kuttan Pillai (1980)**[14], where again the power of search warrant under s. 91 and 93 of Cr. P. C was under challenge. It was contended that it is violating the fundamental right under Art. 20 (3) of Constitution of India. Supreme Court held that general warrant for searching and seizing listed documents would not entail invasion of privacy even if the search did not yield any result because of counter availing state interests. The Court observed that this is not infringing fundamental right.

The power to gather evidence is extended with the use of advanced techniques. After search and seizure, collecting saliva or blood sample was practiced. But with scientific inventions, brain mapping and polygraph tests or lie detector test was conducted by the police. Whether the evidence generated after the reports of such tests invade the fundamental right under Art. 20 (3) i.e. self-incrimination. These tests can result into invasion of privacy of the person as

[12] M.P. Sharma v. Satish Chandra, District Magistrate, (1954) SCR 1077. P. 1096-97
[13] Pooranmal v. Director of Inspection (Investigation) of Income Tax, New Delhi AIR 1974 SC 348
[14] V.S. Kuttan Pillai v. Ramkrishnan AIR 1980 SC 185

person may lose his freedom or right. The same issue was decided in case of Selvy (2010).

Gathering evidence by using advanced techniques was under scrutiny. In **Selvy (2010)**[15] Supreme Court held that use of narco-analysis, brain mapping and polygraph tests on accused, suspects and witness without their consent is unconstitutional and violation of Right to Privacy. The court referred various decisions given by Hon'ble Supreme Court on Right to Privacy. It had considered the decision given in R (on application of S) v. Chief Constable of South Yorkshire[16], UK, where the Court of Appeal held that retention of fingerprints and DNA samples did not violate the right to privacy provided under Art. 8(1) of the convention as it is justified under Art. 8 (2).

The Judges said, evidence obtained through compulsion is not admitted in evidence. Therefore as these technics produces results which are obtained by compelling the person to go through the test, they violate the right against self-incrimination. Article 20(3) of the constitution protects an individual's choice between speaking and remaining silent, irrespective of whether the subsequent testimony proves to be inculpatory or exculpatory."[17] The bench said, "Article 20(3) aims to prevent the forcible conveyance of personal knowledge that is relevant to the facts in issue. The result obtained from each of the impugned tests bear a testimonial character and they cannot be categorised as a material evidence."[18] The CJI said, "It is our considered opinion that subjecting a person to the impugned techniques in an involuntary manner violates the prescribed boundaries of privacy and it would be unwarranted intrusion into personal liberty.[19]" Here the Court held in favour of the person and held that gathering of evidence by employing advance techniques amount to breach of Right to Privacy.

It is important to note that when the R (on application of S) v. Chief Constable of South Yorkshire case was referred to Court of Justice of European Union by the Appellant, (discussed below by the researcher) as UK was part of European

[15] Selvy v. State of Karnataka, 2010 (7) SCC 263.
[16] R. v. Chief Constable South Yorkshire, (2003) 1 All E R (148) (CA)
[17] Selvy v. State of Karnataka, 2010 (7) SCC 263.
[18] Selvy v. State of Karnataka, 2010 (7) SCC 263.
[19] Selvy v. State of Karnataka, 2010 (7) SCC 263.

Union at that time, the Court of Justice of European Union held that retention of fingerprints and DNA samples after the person is acquitted by the court is breach of right to privacy.

5.2.2.2 Right to Personal Liberty

Right to privacy was judged in the context of personal liberty of the person and decision was given by Supreme Court in following case. Right to Privacy was not well-known till the decision in Kharak Singh was pronounced by the Hon'ble Supreme Court. This was decided for the first time in Kharak Sing's case and the first tort explained by Prosser i.e. intrusion upon person's solitude was upheld by Hon'ble Supreme Court.

In **Kharak Singh (1963)**[20], the Police Regulations in UP were challenged. The petitioner was challenged in dacoity but released as there was no evidence against him. The police opened history sheet against him. Definition of history sheets was provided in Regulation 228 of Chapter XX of U. P. Police Regulations[21] as personal records of criminals under surveillance. He was put under police surveillance. Under the Regulation 236 of Police Regulation UP, Surveillance involves—a. Secret picketing of house or approaches to the houses of suspects, b. domiciliary visits at night, c. periodical enquiries by officers not below the rank of sub-inspector into the repute, habits, association, income, expenses or occupation, d. the reporting by constables and chaukidars of movements, absence from the house, e. the verification of movements and absence by means of inquiry sips and also f. collection and record on sheet of all information bearing on conduct[22].

The Petitioner challenged the constitutionality of Chapter XX of UP Police Regulation and in particular Regulation 236. It was also contended by the petitioner that surveillance, and untimely visits of police breached his right to privacy. The case was decided by six judge bench. In majority judgement, the U.P. Police Regulation was held valid. The petitioner challenged that his right to privacy is violated by late night knock on his door.

[20] Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295
[21] U.P Police Regulation and Police Act, 1861.
[22] U.P. Police Regulation and Police Act, 1861.

When this case was decided, the principles governing the inter-relationship between the rights protected by Art. 19 and the right to life and personal liberty under Art. 21 were governed by the judgement in Gopalan[23] case as it considered the right protected under each article as distinct right and not overlapping. The majority judges held because of picketing, the freedom to move freely, guaranteed by Art. 19 (1) (d) was not infringed.[24] It was held that, Art. 21 is not applicable in this situation as right to privacy is not guaranteed in our constitution. So if the police is only ascertaining the movements of the person, it is one of the method, and so is not breach of fundamental right under the constitution.[25] So in Kharak singh also court held that right to move freely under Art. 19 (d) is distinct right and has no relation with right to life under Art. 21.

But domiciliary visits under S. 236 (b) was held invalid as against the right to life protected under Art. 21. Court held that, the word 'personal liberty' shall not be construed to exclude the invasion and intrusion in man's personal security as his right to sleep is a necessity for his existence even as an animal. The court held that in Preamble the words 'dignity of individual' are used and protection of it ensures the full development of a person. The court held that the words personal liberty shall be construed in a reasonable manner and in the same sense which would promote and achieve those objectives.[26] It was held by majority that right to life is infringed by the domiciliary visits at night. But the decision was not based on right to privacy.

But in minority judgement given by Subba Rao and Shah JJ that out of other surveillances, surveillance by domiciliary visit was held against the person's right to privacy under Article 21. The Hon'ble Judeges held in minority that by untimely visits, even in night to the house of a person breaches his right to privacy. While discussing the restraints on free movements, the court held that restraints can also be created by certain conditions apart from scientific methods. It was held that personal liberty lies in freedom from encroachment on the personal life of any person and not only from the freedom of movement. The

[23] A.K. Gopalan v. State of Madras, (1950) AIR 27.
[24] Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR(1) 332, para 340
[25] Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR (1) 332p. 351
[26] Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR(1) 332Pp. 347-348

court also reiterates that right to privacy is essential part of personal liberty even though it is not declared specifically by the Constitution.

The court explained that person's own home is very sacred place which provides him rest, physical happiness and security and peace. It is his 'castle'. His home, where he lives with his family, protects his privacy from encroachment by society. The court has stated that what is opined by Frankfurter J., in Wolf v. Colorado [(1949) 238 US 25] about importance of security of one's privacy against arbitrary intrusion by the police, is also applicable to Indian home. The Court held that physical encroachments on his private life would affect it in a larger degree than the physical restraints on his movements. Interference with the privacy is harmful for his health. Therefore it was held that, "We would, therefore, define the right of personal liberty in Art. 21 as a right of an individual to be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures. If so understood, all the acts of surveillance under Regulation 236 infringe the fundamental right of the petitioner under Art. 21 of the constitutions."[27]

First time it was discussed that whether Right to Privacy could be implied from existing fundamental rights. In a limited way, Hon'ble Supreme Court recognised that Right to Privacy exists and included in Art. 21-Life and liberty of the person. The ratio of Kharak Singh ruled the scenario for more than ten years till in Govind's case Supreme Court held in favour of the right.

In **Govind (1975)[28]**, the Supreme Court assessed more elaborately the right to privacy. The petitioner has challenged the Madhya Pradesh Police Regulation-855 and 856 made under s. 46 (2) (c) of M.P. Police Act, 1961. The constitutional validity of regulation which provides surveillance was challenged. Regulation 855 provides that on information, if the District Superintendent believes that a particular individual is leading a life of crime and the behaviour of that individual show determination to lead a life of crime, that individual's name may be ordered to be entered in the surveillance register and

[27] Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR(1) 332 p.358-359
[28] Govind v/s State of Madhya Pradesh AIR 1975 SC 1378

she would be placed under regular surveillance. Regulation 856 provides that such surveillance may consists of domiciliary visits both by day and night at frequent but irregular interval.

The said Regulation was challenged on two grounds, a. Regulation is not framed under s. 46 (2) (c) of Police Act, 1961 and have force of law, b. even if they are framed under section 46 (2) (c) of Police Act, 1961, provisions regarding domiciliary visits offended Art. 19 (1) (d) and Art. 21.

The court upheld the regulation. It was ruled that regulation is 'procedure established by law', and therefore it is not violating the Art. 21. The Court had observed that Constitution makers were aware of the values propounded by Brandeis J in Olmstead[29] relating to spiritual nature, feelings and his intellect. They were also aware about the pain, pleasure and satisfaction from the use of material things. To protect these spheres from the government actions, they have conferred certain space where he should be let alone. [30]

The court accepted the fundamental right to privacy in limited scope emanated from Art. 19(1) (a), (d) and 21. It was also held that this right is not absolute and reasonable restrictions can be placed thereon in public interest under Art. 19(5). The fundamental right can be overridden by the compelling state interest. It was held, "There can be no doubt that privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling state interest test. Then the question would be whether a state interest is of such paramount importance as would justify an infringement of the right."[31]Court had considered the decisions given in cases of Wolf v. Colorado and Griswold along with the European Convention regarding Right to Privacy. Mathew, J, observed that "Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right of privacy is itself a Fundamental Right, the fundamental right must be subject to restriction

[29] Olmstead v. United State, (1928) 277 US 438.
[30] Govind v/s State of Madhya Pradesh AIR 1975 SC 1378. P.155
[31] Gobind v/s State of Madhya Pradesh AIR 1975 SC 1378

on the basis of compelling public interest."[32]The court denied the claim of the petitioner.

In changed political scenario, to collect the information about the political rival, tapping of the telephone of him was practiced widely. The same action was practiced by police to gather evidence also. Action of the state by tapping of the means of communication, telephone at that time, was under scrutiny that whether such action implies to invasion of privacy of an individual.

5.2.2.3 Right to Privacy of Communication

The Supreme Court's decision in Govind reintroduced the right to privacy into Indian legal system though the regulation was held valid. This protection was extended to another aspects like communication privacy over the period of time. The protection against tort of encroaching the property was extended by recognising the encroachment on communication by one individual to another through telephonic communication. Though the protection was not given under 'Right to Privacy' but the issue of obtaining tapping of telephonic conversion during investigation was considered.

In **R. M. Malkani (1973)[33],** where the police officer, during investigation of case, with the authority of petitioner, attached the tape recorder to his telephone and obtained the evidence of illegal gratification. It was contended by the petitioner inter alia that the evidence of telephonic conversation is obtained illegally in contravention of S. 25 of Indian Telegraph Act and therefore inadmissible as evidence. S. 25 provides that if a person intending to intercept or acquaint himself with contents of any message damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other things whatever, being part of or used in or about any telegraph or in working. It is punished with imprisonment or with fine or with both. The Court observed that the tape recorder was attached to the telephone with authority of the petitioner and therefore there is no breach of the provisions of S. 25 of Indian Telegraph Act and evidence obtained is admissible. The petition was dismissed but Supreme Court stated that telephonic conversation of an innocent person would

[32] Gobind v/s State of Madhya Pradesh AIR 1975 SC 1378 para.31
[33] R.M.Malkani v/s State of Maharashtra AIR 1973SC 157

be protected by the courts against wrongful or high-handed interference by tapping of the telephone conversation by the police. Though it was not linked to right to privacy but the protection was given on the same line as tapping of the telephone is also considered as breach of privacy.

This aspect of privacy, is a personal communication, and by intrusion and invasion on it is by tapping of the telephone was covered under PUCL's case in detail. Earlier the same issue was discussed in R. M Malkani but as the tapping was done with the permission of the owner, the protection was denied. The question whether tapping of telephone is constitutional was discussed in detail in the case of **People's Union for Civil Liberties (1997)**[34]. Telephone tapping is permissible in India under S. 5(2) of the Telegraph Act, 1885. The writ petition was filed by voluntary organisation due to mass tapping of the telephones under S. 5(2) of Telegraph Act, 1885 and challenged the constitutional validity of the same.

This section lays down the circumstances and the grounds when an order for tapping of telephone may be passed. The constitutionality of this section has been questioned, and also no procedure for making the order is laid down therein. On an analysis of s. 5(2), the Court has concluded that "the first step is the occurrence of any public emergency or the existence of any public safety interest. Thereafter, the competent authority under s. 5(2) is empowered to pass an order of interception after recording its satisfaction that it is necessary or expedient to do so in the interest of states etc. same as provided under Art. 19 (2). The authority passing it must be satisfied that the situation is covered under the provision, then the said authority may pass the order for interception of messages, by recording reasons in writing for doing so.

S. 5(2) provides for situations under which the power of interception of messages/conversations can be exercised. But the substantive law as laid down in S. 5(2) must have procedural backing so that the exercise of power is fair and reasonable. Under s. 7(2) (b) of the same Act provides that Government may

[34] People's Union for Civil Liberties v/s Union of India AIR 1997 SC 568, (1997) 1 SCC 301

prescribe the rules for taking precautions for prevention of improper interception.

But it was highlighted in this case that no such rules were made by Central Government at that time under s. 7 (2) (b) of the Telegraph Act, 1885. (These rules were drafted in the year 1999 after the Supreme Court decision in the case **PUCL (1997)**[35]. The Court expressed the view that "These rules provide the solid base for the interference of privacy rights for "intrusion upon a person's solitude or seclusion" and 'information collection'. In absence of just and fair procedure for regulating the exercise of power under S. 5(2) of the Act, it is not possible to safeguard the rights of the citizens guaranteed under Articles 19(1) (a) and 21 of Constitution of India.[36] In the course of its judgement, the Supreme Court referred to the International Covenant on Civil and Political Rights, 1966[37] to which India is signatory. Article 17 of the Covenant provides for right of privacy and this provision is not conflicting with Article 21 of Indian Constitution. The Court has accordingly interpreted Article 21 inconformity with the International Law.

After considering the judgements of Supreme Court in Kharak sing and Govind, the Court has ruled in the instant case 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 in a given case constitute a right to privacy, protection under Article 21 is extended to them. This right cannot be taken away or lessened except provisions or procedure provided under the law.[38]. The Court stated that whether the person can claim such right or not, only depends upon the facts and circumstances of the case. But the person has right to hold a telephone conversation in the privacy of one's home or office without interference. If he does so he can claim as his 'right to privacy'. The Supreme Court has held that conversations on the telephone have an intimate and confidential character being an important facet of personal life of an individual. The court held that such conversations can be protected under Right to privacy.

[35] PUCL v. Union of India (1997) 1 SCC 301
[36] PUCL v. Union of India (1997) 1 SCC 301
[37] https://www.ohchr.org/en (Last visited on December 20, 2019)
[38] PUCL v. Union of India (1997) 1 SCC 301.p. 311.

Therefore tapping would infringe Art.21 of the Constitution of India unless it is permitted under the procedure established by law.[39]

The Court has recognised that the conversation on telephone is integral part of person's life and it should not be encroached or invaded without justifiable state interest. In most of the cases above, the state's power to access information by search and seizure or by tapping was challenged. But unauthorised disclosure of information after accessing it by private parties is also breach of right to privacy of an individual. This aspect was also considered in cases discussed below.

5.2.2.4 Right to Disclosure of Information

Disclosure of personal information is one aspect where courts guarded the right to privacy. Claims for unauthorised disclosure of personal data or information which breaches the right to privacy are often heard and decided by the Court.

Disclosure of information is often done by the media-newspapers or publishers after accessing the personal information to exploit the news. The privacy of person is invaded as reach of the media is vast in comparison to the disclosure through a person.

The invasion by press i.e. publishing the information was raised and discussed in **R. Rajgopal (1994)[40]**. The dispute was regarding the freedom of press and the privacy. The autobiography of a prisoner-a hard core criminal- was to be published by magazine. For this purpose it was alleged that the prisoner has given power of attorney to the publisher. The prison authorities took the objection as names of many high officers were involved in the book. The publisher published three parts in three issues on the magazine. Publisher was under apprehension that police may raid the press and damage the press as it was done on earlier occasion also.

The authorities took objection on the ground that the prisoner had not given any authority to the publisher to publish his autobiography and power attorney is false. Publishers approached Supreme Court for protection of their right under Art. 19 (1) (a), freedom of Speech and expression. The respondents alleged that

[39] PUCL v. Union of India (1997) 1 SCC 301. P. 311
[40] R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632

the names mentioned in the autobiography amount to defamation of the officers. Unauthorised writing of autobiography of one person is breach of right to privacy of that citizen.

The Supreme Court has stressfully pointed out that right to privacy has acquired the status of fundamental right. It is included in Art. 21 as 'right to be let alone'. A citizen has "right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing, and education among other matters."[41] The court had tried to reconcile the two fundamental rights, right to privacy and right to speech and expression, which may be in conflict at times. The Court put forward some propositions inter alia:

1) Nobody can publish any personal information, whether critical or praising him or true or not without seeking permission of the person relating to whom the information is published. If anybody publishes it without permission, he is liable for damages as he is violating the right to privacy which is covered under Art. 21.
2) If such personal information is available in public domain or in public records including court records, permission is not required and publication of personal information is exempted as right to privacy is not attached to it."[42]
3) No action for damages in breach of right to privacy can lie against the public officials, if they are discharging their official duties. Otherwise the person has to prove that the publication was false or actuated with malice or personal animosity."[43]
4) State or its officers are not empowered under any law to prohibit or impose restraints on press/media before publication of any information.

The Court had made it clear that the principles above mentioned are only the broad principles. They are neither exhaustive nor all-comprehending. It was rightly pointed out by Mathew, J; that this right has to go through a case-by-case development.

[41] R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632
[42] R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632, p. 649-650
[43] R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632, p.649-650

We can observe the evolution of the concept 'Right to Privacy' from Kharak Sing[44] to Rajgopal[45], as in earlier case physical privacy was emphasized, and in later case the issue was of reputation of the officers involved and alleged defamation by disclosing information. So the privacy other than physical privacy was targeted.

But where disclosure of information is necessary to protect the fundamental right of another person or the interest of the public then court did not hesitate to hold against the right to privacy. It was evident in **Mr. X (1999)**[46] where the applicant's blood was to be transfused to another but he was tested HIV (+) at the respondent's hospital. On the account of disclosure of this fact, the appellant's proposed marriage to one A, which has been accepted, was called off. Moreover he was severely criticised and was ostracized by the community. The appellant approached the National Consumer Dispute Redressal Commission for damages against the respondents on the ground that the information required under medical ethics, to be kept secret, was disclosed illegally and therefore, the respondents were liable to pay damages to the appellant. The commission dismissed the petition on the ground that the appellant should seek his remedy in the civil court.

Before the Supreme Court the appellant contended that the principle of "duty of care" applicable to persons in medical profession included the duty to maintain confidentiality and that the said duty had a correlative right vested in the patient that whatever came to the knowledge of the doctor should not be divulged. The appellant added that for violating that duty as well as for violating the appellant's right to privacy, the respondents were liable for damages to the appellant.

The Supreme Court, while rejecting the appellant's contentions, held that the right to privacy is amassed from Article 21 and other Fundamental Rights read with the Directive Principles of State Policy. The Court observed that this Right may arise out particular relationship mainly from contract but also including, commercial, matrimonial or even political relationships. Doctor-Patient

[44] Kharak Sing v/s /State of Uttar Pradesh AIR 1963 SC 1295
[45] R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632
[46] Mr. X v. Hospital Z AIR 1999 SC 495, (1998) 8 SCC 296

relationship apart from being commercial, also includes the confidence. Doctors are morally and ethically bound to maintain confidentiality under their professional ethics. In such situation, disclosure of truth about private facts may amount to an invasion of the right of privacy. This may result into the clash between rights of two persons. Court observed that in this case, one person's 'right to be let alone' with other person's right to be informed is clashed. The right, however, is not absolute and may be lawfully restricted for many purposes including protection of rights and freedom of others. The Court held that in clash of the fundamental rights of two persons under art. 21, the right which promotes the public morality or public interest, will be enforced through court"[47] [48] The claim of the petitioner was rejected.

The information regarding the DNA reports is sensitive personal data. How far this sensitive information be disclosed and whether the person can be compelled to give sample for testing. These question was discussed in **Sharda (2003)**[49]. In the divorce proceedings, the medical examination was ordered for proving the contention of the party. The appellant refused taking umbrage of Right to Privacy under Art. 21. High court decided against the appellant and appellant moved to Supreme Court. It was held that in divorce proceedings, to arrive at proper decision, an order to undergo medical examination on strong ground of necessity to establish a contention. It is necessary to prove or disprove the allegation made. It was held by Supreme Court that if the umbrage of Right to privacy under Art. 21 is taken for avoiding the medical examination which is necessary to evaluate the claims made and defence provided, it is impossible for court to arrive at some definite conclusion on the issue. Moreover it is not absolute right. Court refused to grant relief in favour of the wife.

The important aspect of privacy of individual, i.e. informational privacy was first time traced and tested in true sense by Supreme Court in the case of **Canara Bank** [50] (2005). In this case s. 73 of Indian Stamp Act, 1899 was incorporated by Andhra Pradesh Act, 17 of 1986 by amending the central Act. S.73 of Indian Stamp Act, 1899 empowered the collector or any person authorised by him to

[47] Mr. X v. Hospital Z AIR 1999 SC 495, (1998) 8 SCC 296 p. 305-307
[48] Mr. X v. Hospital Z AIR 1999 SC 495, (1998) 8 SCC 296
[49] Sharada v. Dharampal,(2003) 4 SCC 493.
[50] District Registrar and Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496

inspect the registers, books and records, papers, documents, and proceedings in the custody of any public officer 'to secure any duty or to prove or would lead to the discovery of a fraud or omission. This section was amended by Andhra Pradesh Act, 1986, under which along with the powers conferred under original section, the collector or any other person authorised by him can seize and impound them if it is necessary under proper acknowledgement. The person who is authorised by collector can seize the documents accessed after giving notice.

Statement of Object and Reason to the amended Act provides that as under s. 73 of Indian Stamp Act, 1899, power of seizure and impounding was not provided, the state loses the revenue of stamp duty as documents are not properly stamped or inadequately stamped. Writ petitions were filed by challenging the provisions on the ground that it is ultra vires to Constitution and inconsistent with Stamp Act and breaching the fundamental right under Art. 14 of the Constitution of India.

High Court of Andhra Pradesh struck down the amended s. 73 of the Act on grounds inter alia that amended s. 73 is inconsistent with other provisions of Act, provision is arbitrary and unreasonable and hence violative of Art. 14 of Constitution. The decision was challenged in Supreme Court on the ground of constitutionality and right to privacy of the persons whose documents are in custody of Banks. After verifying the privacy judgements given by Supreme court of India and United State and privacy right under international conventions, Supreme Court held that, as the ratio in Govind [(1975) 2 SCC 148]is accepted, and in later cases it was held by the court that the right to privacy deals with "persons and not places", the other argument that privacy deals with places and not persons as propounded in Miller[425 US 435 (1976)] cannot be accepted. Even if the documents which are no longer at the customer's house and have been voluntarily sent to bank, they should remain confidential. Unless there is a material which shows to the Collector that documents in possession of bank are lacking in sufficient stamp duty, or there is fraud or omission for payment of the stamp duty, search of the document or taking extract of the document is not valid action. The material must be reasonable for forming an opinion to Collector for issuing an order for search. This safeguard

shall be followed while 'action can be taken after forming an opinion' is provided in the law.

Commenting on the ground of unreasonable and arbitrary exercise of power the court held that, the impugned provision, s. 73 empowers the Collector to authorise "any person" whatsoever to inspect, to take notes or extracts from the papers in the public office which is wrong on the basis of the principle of excessive delegation. For delegation of such power, the guidelines to exercise the powers shall be in the Act. Here guidelines are absent. More importantly, as it allows the non-governmental persons to access the facts relating to the customer's privacy, it is an unreasonable encroachment in to the customer's rights. The Court held that, providing access to "any person" is a serious defect and it is unenforceable on this basis. The court also expressed the opinion that the state must clearly define the officers by designation by naming the officers not below a particular rank in the official hierarchy, or expressly define the scope of delegation."[51]

This judgement is important regarding the right to privacy in India. The court recognised that the right to privacy is available not only under Constitution of India but it is provided under Universal Declaration of Human Rights and other international Covenants also. Here in this judgement, Supreme Court differ from US decision in Katz[52], which provides privacy under Fourth Amendment is attached to places and not to person. The Supreme Court declined to follow Miller[53] and held that privacy attaches to person and not places so if the papers, records, documents are in possession of bank which are, deposited by the person, person has reasonable expectation that such documents will be used for the purpose for which they are taken. Parting of the information to the bank does not mean that person has lost his privacy interest in the document and information contained in it. He reasonably expects that the document and information placed in custody of bank will not be accessed by any third party. The court held that while protecting the state interests, the state shall take precaution that information shall not be accessed by private entity.

[51] District Registrar and Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496
[52] Katz v. United States(1967) 389 US 347
[53] Unites States v. Miller (1976) 425 US 435

The publishing the information even though the information is about the achievement of the person is covered in Right to Privacy. In **Indu Jain,**[54] (High Court of Delhi, 12th October,2007), a suit for injunction order to prevent the defendants from publishing the Plaintiff's name in Forbes list of Indian billionaires on the grounds of a breach of right to privacy. The respondents claimed that the name is published to give information to public and they have fundamental right of speech and expression. The public has interest in having the information.

Court ruled that "A public figure is one who by his standing, accomplishment, fame, mode of life or by adopting a profession or calling gives the public a legitimate interest in his doings, affairs and character. The standard to be adopted for assessing as to whether the published material infracts the right to privacy of any individual is that of an ordinary man of common sense and prudence and not an out of ordinary or hyper-sensitive person".[55] It had also defined the 'public interest' that "public interest in the matter published has to be more than idle curiosity".[56]

The Court refused to grant injunction against the publication on the ground of freedom of expression and right to information of public. The court noted that right to privacy can be claimed only against state instrumentalities, but it hinted in the order that despite the absence of any statute granting a right to privacy, the guidelines provided by Hon'ble Supreme Court in R. Rajgopal develop such right.

Right to Privacy in relation to the publishing the material by making the television serial is discussed in Managing Director, **Makkal Tholai, (2007)**[57]. A case was concerned about an application filed for injunction order by the respondent, a widow of infamous outlaw Veerappan, against the defendants, in order to prevent the defendants from telecasting a television serial on his life. The application contended that depicting the private life of Veerappan in the serial is against the right to privacy of the respondent and her daughters.

[54]Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006
[55] Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006
[56] Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006
[57] Makkal Tholai v.Mrs. Muthulakshmi, (2007) 5 M.L.J. 1152 at http://indiankanoon.org/doc/47400

While deciding right to privacy of person, court referred the judgement in case of Rajgopal[58] which provides that a person has right to protect privacy of his own, his family, marriage, procreation etc. and nobody can publish anything without his consent. The Court recognised the right to privacy of the respondent balancing it with freedom of press under Art. 19 (1) (a), and allowed the defendants to produce and telecast the serial on undertaking that it will not telecast personal life of Veerappan. Courts generally examine a) the existence of person's right to privacy, b) the conduct of another causing a breach in to the privacy; and c) whether such breach is legally permissible.

Whether disclosure of the personal information of the person, who earlier led a notorious and infamous life amount to breach of right to privacy. This sensitive issue was discussed in one of the leading cases on Right to Privacy of **Phoolandevi'.**[59]' In this case she had contended that the film 'Bandit Queen' falsely portraying her, because of which her Right to Privacy was breached. The film was directed by Shekhar Kapoor mainly on the basis of biography 'India's Bandit Queen: The True Story of Phoolandevi', of infamous lady dacoit Phoolandevi by writer Mala Sen and prison diaries and other material. The film starts with the caption, 'This is true story'. It was released in 1994, and received many awards. Phoolandevi earlier made an application for restraining defendants from exhibiting the film publicly or privately. Court ordered not to exhibit the film publicly or privately. But the film was shown in private theatre in Delhi as she contended.

She contended that some of the incidents like rape of Phoolandevi when she was a child or her attendance at the time of massacre in the Bahmai village was wrongly depicted. She also contended that the facts presented in the film are not explained in the book by Mala Sen and are false. She contended that defendants have no right to mutilate or distort the facts as these facts are not mentioned in the book or prison diaries on which the film is based. She said that due to this wrong depiction, her Right to Privacy is breached. It was argued on behalf of plaintiff that Covenant on Human Rights provides for Right to Privacy.

[58] R. Rajgopal v/s State of Tamilnadu AIR 1994 632
[59] Phoolan Devi v. Shekhar Kapoor and Ors. 57 (1995) DLT 154, (1995) (32) DRJ 142.

The defendants argued that Phoolandevi is public figure and famous and right to privacy is not available for famous person. She had given many interviews to the journalists because of being public figure about incidents in her life and therefore the facts are known to public and are in public domain. So making a film on such material is not breach of privacy.

The Court considered the various material on record and referred the opinions in cases Gobind (1975) and Rajgopal (1994) by the Supreme Court. The court held that "though she is public figure, she has every right to protect her personal life by defending against the activity to enlarge the events of rape on her, or her exploitation, exhibiting nudity etc. which brings shame, humility and remembering the events of past again. The woman who was raped and gang raped in past, if she is still alive, she has right that such events shall not be made public. Individuals need a sanctuary where they can live outside of public control."[60]

It was held by referring the decision in Rajgopal(1994)[61] that "right to privacy is implicit in Right to Life and liberty under Art. 21. Giving interviews about the facts of her past does not amount that the facts or matters are in public domain as held by Supreme Court in Auto Shanker's case. Therefore Plaintiff has a right to privacy and exposing the personal facts of the plaintiff by making the film amounts to breach of right to privacy of the plaintiff[62].

The parties reached settlement outside the court.

Whether right to privacy is available to public figures, when their personal information is published. The issue is important as all types of media look forward to catch some gossip about them. The issue of availability of privacy of public figure erupted in the case of **Maneka Gandhi[63] (2002)**. It was contended by Mrs. Maneka Gandhi that incidents about strained relationship of Ms. Maneka Gandhi with her mother-in-law, Mrs. Indira Gandhi, Prime Minister of India were included in autobiography written by renowned journalist Mr. Khushwant Singh, which he intended to publish and it is breach of her right to

[60] Phoolan Devi v. Shekhar Kapoor and Ors. 57 (1995) DLT 154, (1995) (32) DRJ 142.
[61] Rajgopal v. State of Tamil Nadu, AIR 1994 632
[62] Phoolan Devi v. Shekhar Kapoor and Ors. 57 (1995) DLT 154, (1995) (32) DRJ 142.
[63] Khushwant Singh and Anr. v. Maneka Gandhi, AIR 2002, Delhi 58

privacy covered under Art. 21. Supreme Court, after considering the material on hand and referring the cases on privacy and other authorities on the right held that fundamental right to privacy is not available to her as publishers are not government. Moreover, personal lives of public figures are always scrutinised by the people and they cannot escape from such scrutiny. Whether they are defamatory, for that purpose she has a right to take action for it in lower court. But there is no right to privacy available in the circumstances.

Courts protected the Right to Privacy under Art. 21 Right to life and liberty. In India, Information Technology Act, 2000 is enacted for the protection of commercial transactions using information technology and internet. As the privacy issues started erupting, the demand for the protection of privacy also increased. Government amended the existing sole legislation by adding certain provisions for protection of privacy. But if we observe the cases decided under Information Technology Act, instead of Right to Privacy of person, actions pertaining to the liabilities of the intermediaries are challenged. The researcher has discussed some of the cases in following paragraph.

5.2.2.5 Right to Privacy under Information Technology Act, 2000

Freedom of Speech and Expression and IT Act, 2000

The case which has challenged the fundamental right under Art. 19 (1) (a) and not fundamental right under Art. 21 is the case of **Shreya Singhal (2015)**[64]**.** Two ladies commented on Facebook, a social media site, about the total closure of Mumbai City after the death of influential political leader. The police arrested both of them under S. 295A of Indian Penal Code and under S. 66A of Information Technology Act, 2000. They were released afterwards and also the cases were dropped which were filed against them. Under S. 66A of Information Technology Act, 2000, law enforcement agencies can arrest and prosecute the person without warrants on the charges. The action raised alarm in the minds of people.

The women filed a petition challenging the constitutional validity of S. 66A of Information Technology Act, 2000 on the ground that it is infringing the

[64] Shreya Singhal v. Union of India, AIR 2015 SC 1523

fundamental right granted under Art. 19 (1) (a), freedom of speech and expression. The only restriction on the right is provided under Art. 19(2). They argued that provisions under S. 66A are very vague to restrict the right to comment on the internet which is covered under right under Art. 19 (1) (a).

Under S. 66 A of IT Act, 2000, if any person who sends message through electronic communication which contain any information which is grossly offensive or of menacing character or the information which he knows it is false but sends it to cause annoyance, inconvenience, danger obstruction, insult, injury, criminal intimidation, enmity etc. or sent for purpose of causing annoyance or inconvenience etc. is guilty. The petitioner contended that the parameters which is restricting the person's right to expression by sending messages using electronic media are vague. Such parameters shall be in consonance with parameters provided under Ar. 19 (2). The government contended mere chance of abuse of the provision may not be a ground to declare the provision unconstitutional. Legislature is best position to fulfil the needs of the people. Also loose language of the provision cannot be the ground for invalidity because law is concerned with the novel ways to disturb rights of the people through internet. So if the statute otherwise is legislatively competent and non-arbitrary it is valid and cannot be declared unconstitutional.

The Supreme Court held that S. 66 A of IT Act, 2000 is capable of all types of communications on internet. The Court found that it does not make any distinction between mere expression of opinion or discussion and the message which cause annoyance to somebody. The law fails to establish the close relationship with the intention to protect public order. The Court further held that commission of an offence is complete after sending the message. It does not distinguish between the sending it to one person and sending it to masses to create public unrest.

The Court held that government failed to show that provisions under S. 66A are for the protection against communication inciting the commission of an offence. The Court observed that acts pertaining to mere causing annoyance, inconvenience, danger obstruction, insult, injury, criminal intimidation, enmity etc. or merely grossly offensive are not the offences under Indian Penal Code.

For the contention of the petitioner that the provision is vague, the Court verified the United States cases and held that, "the statute which does not lay down reasonable standards for defining guilt in a Section which creates offence and which does not provide any guidance for law abiding citizens or authorities and courts, Section which creates the offence and which is vague shall be struck down". The Court was of the opinion that S. 66A leaves many terms vague and undefined and therefore is not valid. Court observed that by providing for annoyance or inconvenience, it restricts many innocent speeches. The court declared in unconstitutional.

Importance of the case is that that it is deciding the rights of the parties relating to freedom of speech and expression. The court narrowed down the exercise of power under such vague provisions fixing the liability on the persons.

Liability of Intermediary

Avnish Bajaj[65] (2005) is the first case which was decided under provisions of Information Technology Act, 2000, relating to the liability of an Intermediary. This case was decided before the Information Technology Act, 2000 was amended in 2008. In this case, the company Bazee.com was facilitating the business transactions by advertising the goods on its website. The customer who wanted to purchase the goods shall contact the sellers listed on the website. Transactions are completed by both the parties and Bazee.com did not have any role. By advertising on the website, it earns the money. On this website, it was found that pornographic video was put for sale by the name, "DPS Girls having fun". The filters of website failed to notice it but in manual checking it was observed. After this it was removed from the website but in between this, some purchasers bought videos. The case was registered against the Managing Director of Bazee.com under S. 292 of Indian Penal Code (advertisement or sale of obscene object) and S. 67 of Information Technology Act, 2000 (causing publication of obscene objects on internet). Delhi High Court came to the conclusion that the Managing Director was prima facie guilty under S.67 of Information Technology Act, 2000 as criminal liability can be charged against

[65] Avnish Bajaj v. State (N. C. T) of Delhi (2005) 3 Comp.LJ.364 Del. 116(2005) DLT 427

the director under S. 85 of IT Act (offences against companies) where director can be held guilty even company is not charged with.

Avnish Bajaj preferred a criminal appeal[66] which was heard after tagged with Criminal Appeal 838 of 2008 and it was held by the Supreme Court that the provisions under S. 85 of Information Technology Act, 2000, the director could not be held liable.

Under the provisions of Information Technology Act, 2000, the liability of intermediary is challenged relating to the matter published on website. The case challenging the action under S. 79 of the IT Act, 2000 (before amendment in 2008) is decided exploring the scope in Visaka Industries Ltd. and Ors[67] (2009).

In this case the court verified the liability of intermediary. Visaka Industries are leading manufacturers for asbestos since 1981. They have seven manufacturing plants and twenty five business offices all over India. The defendant Ban Asbestos used to publish the articles on various issues on website hosted by Google Ind. Pvt. Ltd. The contention of the plaintiff was that the defendant has written certain article containing defamatory matter relating to plaintiff Visaka Industries and the said articles were published on the website run by Google which were observed all over the world. Because of these publication, the reputation of Visaka Industries is harmed as such articles are continuously.

The plaintiff by writing to Google India Pvt. Ltd. requested to remove the content from the website. Google India Pvt. Ltd. has answered it is a subsidiary company of Google Incorporation, US and services available on website of Google are not controlled by it. And it is difficult for them to go through each and every article published on their website so they are not responsible for such publication of defamatory matter.

Complaint was filed under S. 79 of IT Act, 2000 and S. 500, 501 of IPC before Metropolitan Magistrate and summons were issued to Google India Pvt. Ltd. Google India Pvt. Ltd. challenged the decision in High Court. Andhra Pradesh High Court verified the liability of the intermediary which is provided under S. 79 of Information Technology Act, 2000. It was observed that the responsibility

[66] Criminal Appeal No. 1483 of 2009
[67] Google India Pvt. Ltd. v. Visaka Industries Ltd. Crl. P. No. 7207 of 2009

of intermediary is excluded only when such act is committed without the knowledge of him. If he conspires or abet the offence then he will be held liable as he loses his protection under S. 79 (3). Here the High Court found that Google India Pvt. Ltd, did not remove the content even after it was brought to the notice of him. High court found it guilty and dismissed the petition.

After the amendment is carried out in 2008 relating to liability of intermediary, the scope of the responsibility under S. 79 of the IT Act, and IT (Intermediary Guidelines) Rules, 2011 was discussed by the court in **Vyakti Vikas Kendra (2012)**[68]. The case regarding the defamatory statements published regarding His Holiness Sri Sri Ravishankar, owner of The Art of Living Foundation, on blogger.com. This blog was created by the Defendant no.1. The plaintiff no 1. Vyakti Vikas Kendra, India, a Pubic Charitable Trust, is registered Public Charitable Trust which is established to implement and promote the spiritual, educational, social and developmental activities for The Art of Living in India. It filed an action for injunction and damages and also for interim injunction against the defendants.

The court observed that Defendant No. 2 is an intermediary within the definition of S.2 (1) (w) and S. 79 of Information Technology Act, 2000. Under S. 79 (3) (b) of IT Act, 2000, defendant no. 2 is under obligation to remove unlawful content being published through its service. It was also observed that he is also bound to comply with the Information Technology (Intermediaries Guidelines) Rules, 2011. Under Rule 3 (3) along with Rule 3(2), the intermediary is obligated to observe due diligence or publish any information that is grossly harmful, defamatory, libellous, disparaging or otherwise unlawful. Court observed that intermediary shall remove such content within 36 hours of having actual knowledge about such defamatory or libellous content under the rules. Therefore it was ordered by the court to remove all defamatory matter from the website of Defendant no. 2 http:/./blogger.com as well as the defamatory links within 36 hours.

So it can be observed that there are few cases relating to intermediary liability and not for right to privacy. The reason may be that people are still not aware

[68] In Vyakti Vikas Kendra v. Jitender Bagga, 2012 AIR (Del) 180

about the protection of privacy, which is mostly relating to physical privacy, under the IT Act, 2000. Some rights are included in the right to privacy but they are not included or recognised by IT Act, 2000. One such right is right to be forgotten. Courts provided the protection of this right.

5.2.2.6 Right to Privacy as a Fundamental Right

Until 2012, it was debated in the various court cases that whether Right to Privacy is fundamental right or not. Supreme Court decided cases on the basis of this right holding that right to privacy is included in Art. 21, but the issue was not substantially and authoritatively decided. The controversy emerged again when government of India has issued uniform identity card scheme for delivery of benefits and subsidies to people. The scheme was opposed as personal information including biometric information was collected for issuing the cards. The Government has established Unique Identification Authority of India under Aadhaar (Targeted delivery of Financial and other Subsidies, Benefits and Services) Act, 2016[69].

J. K.S. Puttaswamy (Retd.) challenged this collection of personal information under Aadhaar scheme. Many cases have filed in the courts all over India challenging this collection by State.

Whether 'Right to Privacy' is to be considered as fundamental right or not, this question arose again when constitutional validity of Aadhaar framework (uniform biometric based identity card) which government wanted to make mandatory for receiving government services and benefits. It was challenged before three judge bench of Supreme Court by retired High Court Judge, **J. K.S Puttaswamy (2012)**[70]. In this petition the collection and use of biometric and demographic information of an individual under Aadhaar scheme was challenged. It was contended that it is violating the fundamental Right to Privacy and therefore invalid. Supreme Court was asked to decide the validity of Aadhaar Act. The Advocate General of India argued that even though many Supreme Court judgements upheld the right to privacy, but Part III of Constitution does not guarantee this right specifically and separately. Moreover,

[69] Act 18 of 2016
[70] J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012

the larger Supreme Court benches in M. P. Sharma (8 judge bench) and Kharak Singh (6 Judge Bench) also refused to decide in favour of Right to Privacy. As a result of this, the court referred this case to larger bench consisting five judges to ensure "institutional integrity and judicial discipline".[71]

Again on 18 July, 2017, the constitutional bench presided over by Chief Justice of India was of the opinion that this constitutional question shall be placed before larger bench consisting nine judges to decide the status of Right to Privacy authoritatively. The petitioner argued that Right to Privacy is an independent right included under right to life (with dignity) and personal liberty under Art. 21. The Respondent argued that Constitution provides protection for personal liberties which incorporate Right to Privacy in a limited sense.

The bench consisted Kehar C. J, Agrawal J, Nazeer J, Chandrachud J, Nariman J, Bobde J, Kaul J. Sapre J and Chelameswar J. The judgement of 547 pages contains six opinions and many observations. Justice Chandrachud wrote plurality judgement for four judges (Kehar J, Agrawal J, Nazeer J, and himself). Nariman J, Bobde J, Kaul J, Sapre J and Chelameswar J each wrote separate concurring opinion. The main issue before the court was whether Constitution of India protects Right to Privacy.

The court verified the judgements of M. P. Sharma and Kharak Sing, A.K. Gopalan, R.C. Cooper and Maneka regarding jurisprudential correctness of the decisions after these cases. Various aspects of privacy were addressed to the Court for deciding the matter were: "i) existence of right to privacy under constitution, ii) Whether it is protected as separate fundamental right; iii) the doctrinal foundations of the claim to privacy; iv) the content of privacy; and v) the nature of the regulatory power of the state."[72]

Chandrachud J., while writing the plurality judgement, discussed the concept 'privacy' as discussed by Warren and Brandies. While discussing the concept and its development under various legal systems, he referred the doctrines suggested and opinions expressed by the various authors, jurists like Thomson, Posner, Prosser, MacKinnon, Robert Bork, and Alan Westin etc. He also

[71] J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012. P. 6
[72] J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012. P.9

referred the opinions expressed by the Courts in USA from Boyd v U.S (1886) to Florida v. Jardines (2013) and UK from Prince Albert v. Strange (1849) to R. v. Commissioner of Police of the Metropolis (2011) while deciding the cases relating to Right to Privacy. He compared the concept and provisions regarding privacy under Canada, South African legal system apart from United Kingdom and United States and European Union. He marked some observations about privacy in different systems of society.

He mentioned the development of concept 'privacy' in Indian legal system. For which, he discussed in length the opinions submitted in Constituent Assembly while providing for Right to Privacy in Indian Constitution. He discussed in length the interdependency of the fundamental rights under Art. 14, Art. 19 and Art.21 by taking note of the freedoms under Art. 19 and rights under Art. 21. He did so by reviewing the decisions in A.K. Gopalan, R. C. Cooper and Maneka cases. He held that "the dissenting view expressed by J. Subbarao represents the exposition of correct constitutional position. The jurisprudential foundation in M.P. Sharma and Kharak Singh has been a settled principles in law after these years. He held that these principles include firstly, the fundamental rights emerges from fundamental notions of liberty and dignity. But some aspects of liberty as protected under Article 19 do not deprive the protection under Art. 21. Secondly, state's action for invasion of any fundamental right under any law shall not be examined on the basis of the object for invasion but it should be examined on the basis of the effects of such invasion on the rights. Thirdly, Constitutional guarantees in Part III become more meaningful when state action is not arbitrary and is reasonable while exercising the power as per the requirement under Art. 14."[73]

It was held that, "A law within the meaning of Art. 21 must be consistent with the norms of fairness and equality under Art. 14. As a matter of principle, once Art. 14 has a connection with Art. 21, norms of fairness and reasonableness would apply to procedure and law both."[74] It was held that in a same way, right

[73] J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012. P. 23, 24.
[74] J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012. P. 241

to privacy is not independent of other rights and freedoms guaranteed by Part-III of the Constitution.

How this is applied in judicial review, which is strong remedy, in case of intrusion by state, is the important issue in this judgement. "The guarantee of equality is a guarantee against arbitrary state action. State is restrained from discrimination among persons. The arbitrary action of state violates the equality as such action destructs the body and mind of person. The intersection between one's mental integrity and privacy entitles the individual to freedom of thought, the freedom to believe in what is right, and the freedom of self-determination. Above all the privacy of the individual recognises an inviolable right to determine how freedom shall be exercised."[75] The court explained it in the judgement. If the privacy is violated by state action, like exercise of powers of search and seizures, or enacting any law restricting the person then such action or law must be just, fair and reasonable, as it was held in Maneka.

The court had reviewed the decisions given by the Supreme Court on Right to Privacy and discussed various aspects of privacy in those decisions. The Supreme Court has provided protection against the state's power of search and seizure, surveillance, telephone tapping and interception. But the court has discussed the case of Canara Bank[76], in which the court held that the information provided to bank is also protected as privacy is extended to the information provided to the third party. Here the court held that the "privacy attaches to persons and not places."[77] This aspect of privacy, the informational privacy was emphasized by the court in this judgement. Before exploring this the Honb'le court has discussed the concept of privacy.

The concept of 'privacy' is elaborately discussed by the Hon'ble Court in this plurality judgement. The court held, privacy controls the human element which is essential part of human personality. This human element in the personality enables him to take the decisions about his personal life which are also crucial to him. By exercising privacy, he keeps alive his thoughts, beliefs, ideas, preferences and choices while dealing with the society. Privacy of the individual

[75] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 243
[76] District Registrar and Collector, Hyderabad v. Canara Bank,(2005) 1 SCC 496.
[77] District Registrar and Collector, Hyderabad v. Canara Bank,(2005) 1 SCC 496, in this judgement at p. 65.

is an essential aspect of dignity. Privacy is an element of human dignity and it is inalienable natural right. Dignity is intrinsic value and constitutionally protected interest. Dignity and freedom are inseparable interrelating, each one is a tool to achieve other. By exercising the privacy rights, autonomy of his personality is kept intact by individual. According to the Court it comprises the core of the personality of the individual. It helps to take intimate decisions about himself."[78]

Court observed that "while accessing the internet, personal information or data is exposed. This information or personal data may be accessed or disseminated through data mining. This access or dissemination may result into compromising of interests of the individual. Browsing history of the person can reveal information about not only relating to the person but other persons besides him. It is difficult to think all the possible consequences of uses of internet and its harms."[79] In the judgment it was held that as internet and information technology has opened up new avenues for the communication, information of the person is compromised while communicating through internet. Court focused on informational privacy and while discussing the effects of breach or violation of the personal information or data of the individual, the court took notice of dangers of data mining and Artificial Intelligence on privacy of the person. He stressed that state is under positive obligation to protect the privacy of person and also discussed about the negative and positive obligations of privacy. Negative obligations means state is restricted from interfering unfairly in privacy of person. Positive obligations means State is obligated to enact legislative framework to restrict others from interfering with the privacy of the person.

But according to him, "while maintaining balance between data regulation and individual privacy, the issues of legitimate concerns of state interest are to be balanced against individual interests in protection of privacy. He explained that proportionality is essential for taking action by the state. Nature and quality of encroachment by state action on the right of the individual shall not be disproportionate to the purpose of law. He held that by protection of

[78]J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.242-243
[79] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.247-251

informational privacy, human dignity and autonomy to take decisions without interference is protected. He rejected the argument that privacy is an elitist construct."[80]

In this plurality judgement, the Court held that "an invasion of life or personal liberty must meet the three-fold requirement of –i) legality, which postulates existence of law, ii) need, defines in terms of a legitimate state aim, and iii) proportionality, which ensures a rational nexus between objects and the means adopted to achieve them"[81].

The important features of this judgement is it has recognised that Right to Privacy is fundamental right. Also informational privacy is an important aspect of Right to Privacy in this era of communication technology and internet. State shall take care while acting under the authority of law that such law should be just, fair and reasonable and proportionate for the purpose of the action. State shall protect an individual against the invasion of privacy by enacting laws. This is positive obligation of the state. In the negative obligation, State itself shall not invade the privacy of person.

Five concurring opinions were written by other judges separately. Justice **Chelameswar** expressed the view that the scope of the issue challenged is restrictive. According to him, "three questions should be enquired, i) about existence of fundamental Right to Privacy under constitution of India, ii) if it exists, where it can be found, iii) and contours of such right"[82], while deciding the issue challenged.

While answering the first question, he reviewed the ratio decidendi in the cases M. P. Sharma and Kharak Singh. He also considered the judgements in Boyd and other cases by American court. He expressed his opinion that the minority view in Kharak Singh is the proper one and there is right to privacy under Art. 21. According to him, "the Right to Privacy is an essential ingredient of personal liberty and decision in M.P. Sharma is not an authority on right to privacy"[83].

[80] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.252-253
[81] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 254-255
[82] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. p. 269, p.4 in judgement by J. Chelameswar.
[83] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 273, p.7 in judgement by J. Chelameswar.

Court shall interpret the constitution in a manner which would enable the citizen to enjoy the rights guaranteed by Constitution within permissible limits. He pointed out that many rights which were not provided in Constitution are held as fundamental right under Art. 21. So he reiterated the thought that constitution is living document and therefore interpreted accordingly in changing situations.

He also reiterated that rights under Art. 21 shall be compatible with the freedoms provided under Art. 19. He referred decision of Supreme Court in R.C. Cooper where it was held that the rights deprived by any law of a personal liberty under Art. 21, shall satisfy that procedure is fair, reasonable, just and in consonance with 19(2) to 19(6). He revisited the decisions given by US Supreme Court in privacy issues as it held that constitution creates certain zones of privacy-(repose and intimate decision). He referred Gary Bostwick's[84] view that there are three aspects of privacy, 'repose', 'sanctuary', and intimate decision. According to him, "I) Repose-it is freedom from unwarranted stimuli. II) Sanctuary-it is protection from intrusive observation, III) intimate decision –autonomy to make personal life decisions"[85]. On the basis of these three, he verified the freedoms and liberty guaranteed under constitution of India. He held that the state shall not interfere with the person's choices regarding dressing, residence, travel, which are purely private. He stated that freedom of social and political association is guaranteed under Art. 19 (1) (c). He discussed the different contours of privacy which are protected under Constitution of India i.e. right to travel, right of locomotion, right of appearance and apparel etc.

In the end, he held that no right can be absolute and have limitations. He opined that therefore the protection can be given after verifying the nature of privacy interest claimed by the person. No fixed standard can be suggested or applied to each case.

Nariman J. He revisited the decisions of Supreme Court in various cases from M.P. Sharma, Kharak Singh to R.C. Cooper and Maneka for right to privacy in Indian legal system. For reiterating the principle that fundamental rights under

[84] Bostwick, Gary, 'A Taxonomy of Privacy: Repose, Sanctuary and Intimate Decision', (1976) 64 California Law Review 1447

[85] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 301, p. 35 in the judgement by J. Chelameswar.

all the articles are taken in to consideration to test the validity of action, he has cited the case Mohd. Arif [86], where constitution bench of Supreme court held that " in many judgements delivered by Supreme Court, it was held that that Rights guaranteed under other Articles are to be read along with other fundamental rights and so the procedure not only to be just, fair and reasonable, but also the law itself has to be reasonable as Art. 14 and 19. So while interpreting, rights under Art. 21, Art. 14 and 19 shall be considered.[87] He expressed the opinion that right to privacy is human right referring the Art. 12 of Universal Declaration of Human Rights while discussing the judgements of Sharda, Kharak Singh, Rajgopal.. He analysed various provisions of International Conventions, Covenants and treaties relating to right to privacy.[88] He opined that right to privacy developed in later cases like Selvi.[89] He analysed the case laws regarding the development of Right to Privacy and wherein the Right to Privacy was upheld by courts of USA. While discussing the Right to Privacy, he also endorses "Gary Bostwick's conceptual understanding of privacy as encompassing 'Repose, Sanctuary and Intimate decision'[90]. The author suggested that the Right to privacy includes three separate and distinct rights. He classified it in three categories. I) Repose- which involves invasion by state into person's physical body. II) Informational privacy which captures unauthorised uses of personal information. III) Privacy of choice or individual autonomy over fundamental personal choices". [91]

He came to the conclusion that "this right to privacy is inherent to the human being. In Indian Constitution, Right to Privacy is included in Art. 21."[92]

Kaul J. considered the privacy claims against state and non-state entities. He reviewed the article written by Warren and Brandeis on 'Privacy' and observed

[86]Mohd. Arif v. Regisrar, Supreme Court of India and Ors. (2014) 9 SCC 737.
[87] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 376, p. 26 in the judgement by J. Nariman.
[88] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 383-386, p. 32-35 in the judgement by J. Nariman.
[89] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 393, p. 43 in the judgement by J. Nariman
[90] Bostwick, Gary, 'A Taxonomy of Privacy: Repose, Sanctuary and Intimate Decision', (1976) 64 California Law Review 1447
[91] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 445, p. 95 in the judgement by J. Nariman
[92] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 472, p. 122 in the judgement by J. Nariman.

that Right to Privacy may have different aspects. One such aspect of Privacy right is individual's right to control propagation of his personal information. The right against the propagation by the state is protection against surveillance and profiling, and right against the propagation by non-state entities like social networks providers, search engines, e-mail service providers have extensive knowledge of activities of an individual. He recognised that the impact of technology on data generation, collection and use in digital economy compromise the interests of individuals.[93]

He observed the effects of big data on individual and its effects on fundamental right for free speech and expression. He stressed that there is a need to protect against disclosure of certain information to state as well as to private entities. He recognised that there is a need for regulation for storage, processing and use by non-government entities of such information.[94] He observed that privacy is key to freedom of thought[95]. He has recognised that an individual has right to control his personal data, his own life and his presence on internet. But he also cautioned that this right is not absolute"[96] On Right to be forgotten he held that because of technology, the personal information is permanently stored in the device. This becomes difficult when a person chooses to start afresh after some years giving up his past mistakes. The device and its memory never forget and it does not let the individual and others to forget the mistakes the person has committed. In his opinion, every individual has right to re-invent himself and reform him. According to him, privacy makes this possible."[97] On data regulation he agreed with J. Chandrachud, that data protection is a complex process and shall be undertaken by the State carefully. In this process privacy concerns and legitimate state interests shall be balanced properly. It should be observed by the State that after collecting the data and processing it and the scientific an historical research of the such processing, there should be public

[93] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 503-506, p. 7-10 in the judgement by J. Kaul

[94] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 507, p. 11 in the judgement by J. Kaul

[95] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 522, p. 26 in the judgement by J. Kaul

[96] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 528, p. 32 in the judgement by J. Kaul.

[97] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 529, p. 33 in the judgement by J. Kaul.

benefit. He concluded that Right to Privacy is fundamental right which is to be protected against State and non-State actors, but subject to the restrictions specified.

Bobde J. He referred the judgements in M. P. Sharma and Kharak Singh. While discussing the nature of rights protected under the Constitution, he distinguished the rights in fundamental right and common law right as former. Fundamental rights provide remedy against the violation of a valued interest by the state while common law rights can be enforced on one's fellow men and proceeded in the ordinary court of law[98]. He opined that privacy has a nature of being both a common law right as well as fundamental right. But each is enforced in different forum and with different incidence of burden. [99] He observed the content of rights covered under Art. 21 and contents of Right to Privacy. He held that all civilised people felt the necessity of privacy in day to day activities. Expecting privacy starts with when doors are locked, wear clothes, and when we put password for our computers or phones, we demonstrate that we need privacy."[100]

He held that every person is entitled to perform any act in private, and the action is not limited to the actions in his bedroom which is an intimate place. He is entitled to do such acts wherever he goes even in public place. He said that "Privacy has deep affinity with seclusion (of our physical perosna and things) as well as such ideas as repose, solitude, confidentiality and secrecy (in our communications) and intimacy" [101]. But it is not essential to have solitude for privacy. A person is at liberty for not being a part of group ant act for himself alone.

While referring the judgement of Kharak Singh, he explained the term 'life' which is used in it, as is more than mere animal existence. He held that Right to life in Art. 21 touches every organ of the body and therefore cover physical as well as psychological aspects of the person. He observed that privacy is

[98] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.325-326, p. 15-16 in the judgement by J. Bobde.
[99] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 326, p. 16 in the judgement by J. Bobde.
[100] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P.327, p.17 in the judgement of J. Bobde.
[101] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (civil) 494 of 2012. P. 329-330, p.19-20 in the judgement by J. Bobde.

necessary for both aspects of the individual's life, by receiving the same the person attains freedom. He is of the opinion that dignity cannot be guaranteed without the privacy to the person is granted. Dignity and privacy both are essential and the person receives it by birth and shall be granted also during his lifetime.[102] Further he held that the right of privacy is an integral part of both 'life' and 'personal liberty' under Art. 21. Objective of this right is to enable the rights barer to develop her potential to the fullest extent. It is made possible only if this right is exercised in consonance with the constitutional values expressed in the Preamble as well as across part III."[103]

While discussing test of 'privacy' he held that, in practice, value is defined by comparing it with its opposite e.g. freedom is defined as 'absence of restraint'. In the same way, privacy may be understood by its opposite value as 'publicity'.

He provides for the measures for protecting privacy. He held that the action interdicted by a particular law decides the relationship between the right of privacy and the particular fundamental right (or rights) involved. The law which allegedly invaded the privacy of person shall be tested with the same standards by which a law which invades personal liberty under Art. 21. So the action of the state shall be just fair and reasonable while interfering the rights of person. Moreover the tests provided for restricting the exercise of the freedoms shall also be satisfied if the state is invading the Right to Privacy[104]. He concluded that the Right to Privacy is included in Part III of the Constitution.

Sapre J. He discussed the questions which were referred to the court for evaluating the correctness of the views expressed regarding Right to Privacy in the cases of M. P. Sharma and Kharak Singh. He also discussed that whether 'Right to Privacy' is a fundamental Right under part III of Constitution. He discussed the preamble of Constitution and the ambit of Art. 21-Right to life and personal liberty. He associated the right to Privacy with the rights mentioned in the Preamble especially dignity of an individual. According to him, protection

[102] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (Civil) 494 of 2012. P 337-338, p. 27-28 in the judgement by J. Bobde.
[103] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (Civil) 494 of 2012. P. 338, p. 28 in the judgement by J. Bobde.
[104] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (Civil) 494 of 2012. P 347-348, p. 38-39 in the judgement by J. Bobde.

of dignity of every citizen is necessary for the survival of unity and integrity of the nation. According to him, the terms, liberty, equality, and fraternity incorporated in the Preamble are not separate entities. All the terms shall be read in while rights of the citizens are involved. It is therefore a duty of the courts and especially this court to strike a balance between the changing needs of the society"[105]. He reviewed the decisions relating to right to privacy and held that in last many decades, Court has interpreted the constitution keeping in a view the socio, economic, and political conditions in the society.

He opined that right to privacy is natural rights which are available to any living being from the birth. The same is also applicable to any individual. It cannot be alienated.[106] For the definition of right to privacy he relied on the cases decided by Supreme Court especially Gobind v. State of Madhya Pradesh and District Registrar and Collector, Hyderabad and Anr v. Canara Bank and Ors. He also relied on the objectives mentioned in the Preamble as liberty of thought, expression, belief, faith and worship and also fraternity assuring the dignity of individual. He also observed that it emerges from Art. 19 (1) (a) freedom of speech and expression and from Art. 19 (1) (d), freedom of movement throughout the territory of India. and also from the expression "personal liberty" under Art. 21. He held that right to privacy is multifaceted and so it has to be decided case to case basis"[107].

In these six opinions, four common issues were decided positively by all nine judges, therefore they are binding on all the courts in future. The issues are:

i) "The decision in M. P. Sharma which holds that right to privacy is not protected by the Constitution stands overruled.

ii) The decision in Kharak Singh to the extent that right to privacy is not protected by the Constitution stands overruled.

[105] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (Civil) 494 of 2012. P 479-480, p. 7-8 in the judgement by J. Sapre.

[106] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (Civil) 494 of 2012. P 487, p. 15 in the judgement by J. Sapre

[107] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (Civil) 494 of 2012. P 491, p.19 in the judgement by J. Sapre.

iii) The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Art. 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

iv) Decisions subsequent to Kharak Singh which have enunciated the position in (iii) above lay down the correct position in law."[108]

The Puttaswamy's case was based on the issue whether Right to Privacy is fundamental right as validity of Aadhaar Act was challenged on the basis of it. The Supreme Court verified the concepts of 'liberty' 'dignity' enumerated in Preamble and 'freedoms' mentioned in Art. 19 (1) in detail and their interconnection. Their relationship with the right protected under Art. 21 is also discussed. It was held that these rights are to be considered in comparison with each other and with effect of all their parameters on each other. According to the Hon'ble Court, the invasion on privacy shall be dealt with according to the effects of such invasion on the particular right mentioned in the Constitution. While deciding the invasion and mitigating it, the procedure shall not only be 'fair, just and reasonable', but 'proportionate' also, the Hon'ble Court opined.

In e-government, government is providing maximum services to its citizen through computer and internet using information technology. Government has a tendency to collect more information than required under the e-governance projects as it is impossible to foresee all potential future requirements for data. If they need the data for some other purpose than for which the data is collected, they have to undergo the same procedure again.

The government decided to create Aadhaar card-unique identity card containing the information of the residents of India for distributing benefits, subsidies and services. This multi-purpose national identity card used sixteen fields to uniquely identify the person. These fields include fingerprints, and print of iris along with name, gender, residential address, mobile number etc. As this was once-in a life-time data gathering project, every department of the government wanted to use the opportunity to collect some information that it needed. Because of this, large number of data was collected by the government. There

[108] J. Puttaswamy & Anr. v. Union of India & Ors. W.P. (Civil) 494 of 2012. P. 546-547.

are chances that the personal data of individuals may be compromised and privacy of persons is encroached by the government.

The fundamental question relating to 'Right to Privacy' was decided positively by the Supreme Court. The issue relating to collection of personal information or data including biometric and demographic data by the government, that whether such collection is constitutionally valid or not, and whether there is enough protection provided under the Aadhaar Act, 2016 for such data was also decided by the Supreme Court. There were other twenty eight cases involving the same issue were filed in the different courts in India which were transferred to Supreme Court and decided with J.K. S. Puttaswamy's case.

The issue of protection of data or information was decided for the first time. The decision is pioneer in the data protection.

5.2.2.7 Right to Data Protection under Indian law

The data protection was first time invoked specifically in Puttaswamy's[109] case. The informational privacy is known as 'data protection' according to practice in European Union. Data protection is included in right to privacy in India as 'informational privacy' and it was challenged under the breach of Right to Privacy in J. Puttaswamy's case and other 28 cases before various courts in India. All these cases were collectively heard by Supreme Court.

In Puttaswamy, it was argued that the biometric information collected by Government and contained in Aadhaar card has a possibility that the privacy of the individual would be encroached and so validity of Aadhar Act was challenged. Supreme Court emphasized more on informational privacy in this case and it recognised that privacy includes informational privacy also. After this judgement, the J. K.S. Puttaswamy (Retd.)[110]'s case and other 28 cases which were filed in different courts and were transferred to Supreme Court, finally heard by the court on the issue of overall validity of Aadhaar Scheme by five judge bench of Supreme Court. The bench comprised of C.J. Deepak Misra, J. Sikri, J. Khanwilkar, J. Ashok Bhushan and J. D.Y. Chandrachud. Except J.

[109] J. K. S. Puttaswami and Anr. V. Union of India and Ors. W.P. (civil) 494 of 2012
[110] J. K. S.Puttaswamy (Retd.)and Anr. v. Union of India and Ors., and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.

D.Y. Chandrachud (dissenting), others in majority held it valid. J. Sikri authored judgement for C.J. Deepak Misra, J. Khanwilkar including himself.

The petitioners contended that collection of personal, demographic, and biometric information while registering for Aadhaar infringes the right to privacy of the person. It was feared by the petitioners that "personal information provided for getting subsidies and services to government is collected in central data base and it may enable the state to profile the citizens. Also their movements can be tracked and their habits may be assessed and they may be silently influenced. Over the period of time, the State may oppress dissent and influence political decision making. It may enable the state to act as surveillance and authoritarian state." [111]

The petitioners contended that Aadhaar Act is unconstitutional inter alia on the following issues:

i) Aadhaar project under which it is mandatory to give personal data for provision of service, benefits and subsidies creates surveillance state and is thus, unconstitutional,

ii) Aadhaar Act violates right to privacy and is unconstitutional,

iii) Various provisions of Aadhaar Act do not provide for data protection.

A) While examining the first claim of the petitioners, the court examined the object and provisions in Aadhaar Act, 2016. It was observed by the court that "enrolment and authentication processes are strongly regulated so that data is secure. The enrolment agency which collects the biometric and demographic data of individual during enrolment is appointed by UIDAI or by Registrar. The agency employs a certified supervisor, an operator and verifies enrolment and update regulation. Registrar is obligated to use software provided by or authorised by UIDAI for enrolment purposes. The enrolment agencies are empaneled by the Authority. They are given enrolling agency code. The data is encrypted immediately upon capture. The decryption key is with UIDAI solely.

[111] J. K. S.Puttaswamy (Retd.)and Anr. v. Union of India and Ors., and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.

Authentication only becomes available through Authentication Service Agency (ASA) which are regulated by Aadhaar (Authentication) Regulation, 2016."[112]

Regarding the sharing and disclosure of data, it was observed by the court that, "Act prohibits sharing and disclosure of core biometric data under S. 8 and s. 29. Other identity information is shared with requesting agency (AUA) or (KUA) only for limited purpose authentication. The data is transferred from requesting entity to ASA to CIDR in encrypted manner through leased line circuitry using secure protocols. The storage of data templates in safely located servers with no public internet/outlet and offline storage of original encrypted data. CIDR being a computer resources is notified to be a 'protected system' under S. 70 of the Information Technology Act, 2000 by Central Government in December, 2015. Anyone trying to unlawfully gain access into this system is liable to be punished with 10 years imprisonment and fine. The storage involves end to end encryption, logical partitioning, firewalling and anonymisation of decrypted biometric data[113]"

Court verified the structure of legal provisions in Aadhaar Act and concluded that it is very difficult to create profile of a person simply on the basis of biometric and demographic information stored in CIDR. Therefore threat to real time surveillance and profiling by State of an individual submitting the personal data is far-fetched.

B) For second issue the petitioners contended that providing biometric and demographic information is mandatory to receive the subsidies and benefits therefore unless this personal information is provided the individual is not given the benefits which is against the right to privacy of such person. It is provided under s. 7 that proof of Aadhaar number is mandatory for a person willing to receive subsidies, benefits and services. The bargain under this section is an unconscionable and unconstitutional bargain.[114]

[112] J. K. S.Puttaswamy (Retd.)& Anr. v. Union of India & Ors., and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.
[113] J. K. S.Puttaswamy (Retd.)& Anr. v. Union of India & Ors., and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.
[114] S.7,The Aadhaar (Targeted Delivery of Financial & Other Subsidies, Benefits and Services) Act, 2016

For this issue that Aadhaar act, 2016 violates right to privacy, the court referred the various judgements given by itself. It verified scope of Art. 14, 21 as privacy is essential for a person to live life with dignity. The Court has referred the privacy judgement of Puttaswamy and held that "S.7 read with S.5 of Aadhaar Act, 2016 are rationally connected with the fulfilment of the objective contained in Aadhaar Act. Obtaining Aadhaar number is optional and voluntary. Persons living in severe poverty and those who are illiterate will not be in a position to get other modes of identity PAN Card, Passport etc. Even when Aadhaar number is cancelled, it cannot be reassigned again to any individual and there is hardly any possibility to have fake identity. Providing benefits to the persons having Aadhaar card only is duty of government that it goes to deserving persons as the money comes from Consolidated Fund of India, so it is rational to connect the law and object."[115]

It was held by the court that, "privacy is subset of liberty. There are two elements to privacy, subjective and objective element. On subjective level an individual desires to be left alone. On objective level, the individual may make choices which may not infringe rights of others. In Puttaswamy, it held that legitimate expectation of privacy may vary from intimate zone to private zone and from private to public arenas. On web, terrorists wreck the havoc and destruction in civilized countries. Therefore, state interest is national security. State may have justifiable reasons for collection and storage of data apart from the security."[116]

The court also observed that "individual claiming right to privacy must establish that the claim involves a concern about some harm likely to be inflicted upon them on account of an alleged act. Concern should be real and not imaginary or speculative. And also the concern should not be flimsy or trivial but reasonable concern."[117]After observing the provisions in Aadhaar Act, 2016, Court held that concern is not reasonable one as the Act provides for protection of data.

[115] J. K. S.Puttaswamy (Retd.)& Anr. v. Union of India & Ors., and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.
[116] J. K. S.Puttaswamy (Retd.)& Anr. v. Union of India & Ors., and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.
[117] J. K. S.Puttaswamy (Retd.) & Anr. v. Union of India & Ors., and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.

Under Aadhaar Act, 2016, four types of information is collected. i) Mandatory demographic-name, gender, date of birth etc, ii) Optional demographic, iii) Non-core biometric e.g. photographs, and iv)Core-biometric- finger prints, iris. Under s. 2(k) of Aadhaar Act, 2016 definition of 'demographic information' is provided, which excludes sensitive information like race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history. Court held that submission of demographic information including photographs, both mandatory and optional, does not raise a reasonable expectation of privacy under Art. 21 unless special circumstances e.g. of rape victim. This is provided by individual globally to avail benefits. E-mails and phone numbers are also available in public domain.

Court held that "Aadhaar uses demographic information which are not sensitive and where no reasonable expectation of privacy exists. Finger prints and iris scan have been considered to be most accurate and non-invasive, mode of identifying individual which is required for passport, driving license, visa etc. by state use and for mobile phones, lockers, laptops etc. for private use. Person is not asked to submit data about race, religion, caste, tribe, language etc. which is sensitive personal data. So privacy of the person is secured as this data is not stored at enrolling agency but transferred immediately to CIDR".[118]

Court after observing the provisions of the Act, held that "S. 7 provides only for identification for benefits. It nowhere provides that if it fails, no benefit shall be given. Other modes for authentication are permitted. The Circular dt. 24/10/2017, issued by the Authority takes care of the failures for authentication and enrolment."[119] It was of the opinion that purpose of Aadhaar Act, as captured in the Statement of Objects and Reasons and sought to be implemented by S. 7 of Aadhaar Act, is to achieve the stated objectives. The Act is aimed at proper purpose which is of sufficient importance.

* As for the following of the privacy principles, the court held that the data collected is used for giving subsidies, benefits and services provided by the

[118] J. K. S.Puttaswamy (Retd.) & Anr. v. Union of India & Ors., and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.

[119] J. K. S.Puttaswamy (Retd.)& Anr.. v. Union of India & Ors. and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.

government. So purpose limitation principle is followed. S.8 deals with an authentication of Aadhar number and provides that on submission of request from any requesting entity, the Authority shall perform authentication of Aadhaar number and before collecting identity information for the purpose of authentication, the requesting entity shall obtain consent of individual and also to ensure that identity information of that individual is only used for submission to the Central Identities Data Repository (CIDR) for authentication[120]. Under s. 32(3) of the Act, authority is prohibited to collect, store or maintain directly or indirectly any information about the purpose of authentication. So here data minimisation principle is followed.

C) It was also contended that Aadhaar Act, 2016 does not provide for protection of data collected under Aadhaar scheme. The Court verifies the various provisions regarding the protection of data. The Aadhaar (Authentication) Regulation, 2016 and Aadhaar (Data Security) Regulation, 2016 are also verified by the court.

It was observed by the court that Chapter VI of Aadhaar Act, 2016 provides for important aspects pertaining to data protection. S. 28 of Aadhaar Act, 2016, obligation is case on the Authority, as it shall ensure the security of identity information and authentication records of individuals. S. 29 imposes certain restrictions on sharing of core biometric information created or collected under Act or personal identity information. S.30 provides that the biometric information collected and stored in electronic form, in accordance with this Act, and regulations made thereunder, is treated as 'electronic record' and 'sensitive personal data or information'. Explanation to S.30 provides that 'sensitive personal data or information shall have the same meaning as provided under clause (iii) of Explanation to S. 43 A of the Information Technology Act, 2000.[121]

But some provisions which are lacking the data protection are struck down or read down by the court. Some of the provisions which are read down or struck down by Hon'ble Supreme Court are as follows:

[120] S.8, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
[121] S. 30, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

i) S. 33(1) prohibits disclosure of identity information or authentication record except on the order of the court not inferior of the District Judge. Supreme Court held that while passing the order under this section, the person whose information or authentication records are disclosed or released has no opportunity to be heard which is against the principles of natural justice. So it was held that such individual shall be afforded the opportunity to be heard in such court. Provision under s. 33(1) of the Act was read down by the court to this extent.

ii) Under S. 33(2), in the interest of security of nation, on direction of the officer mentioned in the Act, the disclosure of the personal information or authentication record of the person can be done. The Supreme Court held that to avoid possible misuse, a judicial person (preferably sitting High Court Judge) shall be included while deciding it.

iii) S. 47 of the Aadhaar Act, 2016 provides for cognisance of the offences in which the Authority or officer or person authorised by it can lodge a complaint in the court not inferior to that of Chief Metropolitan Magistrate or a Chief Judicial Magistrate. The Hon'ble Court held that the provision shall include that a complaint can be made by any person or victim or whose right is violated apart from the Authority.

iv) Under S. 57, Aadhaar number, for establishing identity of an individual for any purpose it can be used, whether by State or body corporate or person, pursuant to law, for the time being in force, or any contract to this effect. The Court found it impermissible on the two grounds One is that a) it can be misused as the identification can be done for 'any purpose'. It was held that the purpose shall be backed by law for which judicial scrutiny can be available. Moreover it can be used for 'any contract', which was also found impermissible as contractual provision cannot be backed by law. b) Such number can be used by State or 'any body corporate' or 'any person' pursuant to contract with the individual. The court felt that such authorisation may result into commercial exploitation of biometric or demographic information by private entities. Because of the above mentioned reasons, the Court held that it impinge the right to privacy of person and therefore held unconstitutional.

v) S. 2(d) provides for authentication of data. In this provision, 'data' does not include 'meta data' which is provided under Regulation 26(c) of Aadhaar

(Authentication) Regulation, 2016. It was represented by respondents "that 'meta data' includes three types of data, technical data, business data and process metadata. Process metadata include results of various operations e.g. log key data, start time, end time, CPU seconds used etc. therefore only 'process metadata' is included in s. 2(d) as it provides for authentication of data."[122] But court found that it is to be mentioned specifically and so S. 2(d) was struck down.

vi) Under Regulation 27 of Aadhaar (Authentication) Regulation, 2016, the data can be retained for 6 months and then archived for the period of 5 years unless ordered by the court. The Court found it impermissible as the period for retention is too long and it is struck down.

vii) Mandatory linking of bank accounts with Aadhaar was challenged on the basis of art. 14 and 21. The respondents argued that linking of Aadhaar with bank account will help to eradicate black money and money laundering. If the person fails to link Aadhaar, such person would ineligible to access and operate bank account. The court held that "this would amount to forfeiting the account holder's right to access his account which amounts to deprive him from his property and is therefore violative of Art. 300 A of Constitution of India. The compulsion for attachment is not proportionate to the object. It is therefore violate the right to Privacy." [123]

viii) Department of Telecommunication has issued a circular dt. 23/03/2017 and directed that all licensees shall re-verify the existing mobile subscribers (pre-paid, post-paid) through Aadhaar based e-KYC process. Linking of Aadhaar to the mobile number was also challenged as it infringes right to privacy. Respondents argued that non verification of SIM have posed threat in the past. But Court held that "there is no law backing the issuance of such circular for linking of Aadhaar number to mobile and it also fails to meet the requirement of proportionality. So linking of Aadhaar to mobile was held unconstitutional"[124].

[122] J. K. S.Puttaswamy (Retd.). v. Union of India, and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018. Pp. 278-279.
[123] J. K. S.Puttaswamy (Retd.) v. Union of India, and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018. Pp. 511-513
[124] J. K. S.Puttaswamy (Retd.) v. Union of India, and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018. Pp. 520-521

ix) For the admission in educational institutions, the Aadhar is asked. It was challenged. The respondents argued that this is required for verification of the student for distributing scholarships given by government. It was connected with S.7 of Aadhaar Act, 2016 which regulates benefits, services and subsidies provided by government on authentication of Aadhaar data.

The court held that "the term 'benefits' shall be construed relating to welfare schemes. Scholarship is right of student and it cannot be termed as 'benefit' under welfare scheme. Therefore scholarships by CBSE, UGC, NEET shall not be included in it. Moreover art. 21 A of Constitution guarantees right to education and it is fundamental right of children between 6 years to 14 years. Such right cannot be taken away by imposing requirement of holding Aadhaar card upon children. Therefore admission of children cannot be covered under S. 7 of Aadhaar Act"[125].

x) Supreme Court was also asked to decide validity of certain directions from different government departments, which mandated the linking of Aadhaar number. This was specifically in case of linking of Aadhaar to PAN card (for filing Income tax) under s. 139 AA of Income Tax Act. The requirement to mandatorily link Aadhaar number to PAN (Permanent Account Number) was held valid, since it was based on legitimate state interests. The state has legitimate aims to protect its revenue and prevention and interrogation of crime. Provisions for protection of them are proportionate and backed by law. More over digital platforms are vital tool of ensuring good governance in a social welfare state.

xi) For breach of privacy also the Aadhaar act was challenged. But the issue is conclusively settled by the constitutional bench which held that right to privacy cannot be interfered without a just, fair and reasonable law. The Court also clarified that the law must be proportionate to the objective and must serve legitimate aim of the state.

For proportionality, it is clarified that law should have these four aspects. i) It should have legitimate goal for restricting the right. ii) It must have the rational connection, means it must be a suitable means of furthering the goal. iii) There

[125] J. K. S.Puttaswamy (Retd.) v. Union of India, and connected matters, W.P. (civil) 494 of 2012, decided by constitution bench in 2018.

should be necessity and no other effective alternative available. The objective for enactment of Aadhaar is to provide benefits for the down trodden people of the country. These money come out of Consolidated Fund of India. It provides benefits to the person having Aadhaar card only and it is duty of the state that it goes to deserving person. So it is rational to connect the law and object. So Aadhaar Act is constitutionally valid. iv)The right of the holder must not be affected disproportionately. The holder has two fundamental rights, right to privacy and right to food, shelter and employment. Base of both these rights is human dignity. On these basis, Aadhaar Act was held valid.

xii) The court has issued the direction to Central Government that it should enact data protection legislation on the recommended framework of J.B. N. Shrikrishna.

As it is discussed above the protection of personal data is provided by Supreme Court with reference to collection of personal information or data under Aadhaar Act, 2016. Here the collection is for provision of services, subsidies and benefits by government, which was held essential for fair and just distribution of the same. But when personal data or information is collected for services by the government which are not for subsidies, or benefits, the liability of the government is not discussed in the case.

5.2.2.8 Right to be forgotten:

This right is not recognised under Indian Legal System. It is provided under Personal Data Protection Bill, 2019. But Indian courts were recognised this right in some of the cases. The initial case is decided by Gujarat High Court. In Bhanushankar[126], a person was accused of criminal conspiracy and murder. Afterwards, Sessions Court acquitted him and Gujarat High Court confirmed the decision. The judgement was published on internet by State of Gujarat though it was not reportable. He filed writ petition under Art.226, restraining the respondent from publishing online on the basis of 'right to forgotten'. Court held that petitioner failed to prove that he has any injury under Art. 21 and also there is no right to forgotten available in India.

[126] D. Bhanushankar Dave v. State of Gujarat, C/SCA/1854/2015, Gujarat.

Gujarat High Court denied the right but it was held in favour of the person by Karnataka High Court in Vasunathan's[127] case. Here daughter of the person filed an FIR against one man alleging for the offences for compelling her for marriage and forgery. Civil suit was also lodged by her for annulment of her marriage certificate as there was no legal marriage. Subsequently the parties has settled the matter on the condition that criminal case against the man shall be withdrawn. Her father made an application for quashing FIR and Hon High Court of Karnataka allowed it. This said order recorded the petitioner's daughter's name as respondent no. 2 with her full identity details. Petitioner filed an action to remove her name from the record of respondent and contended that name wise search on search engines like Google and Yahoo may reflect the order on result page. There are high chance that the said order may affect the relationship of his daughter with her husband and also her reputation in public image.

After considering the arguments of petitioner, High court directed the respondent to take necessary steps to mask the name. It also acknowledged that right to be forgotten.

The #Me too movement was started against the sexual harassment of working women. But if such allegations are made against an innocent person whose name may appear on the internet then whether such person has right to forgotten? In case of Zulfikar Ahmen Khan[128] Delhi High Court held this in affirmative. In this case, two articles were published by the respondent containing harassment allegations against the plaintiff in 2018. He challenged this publication in court submitting that he is well-known personality in media industry and Managing Director of media house. Due to publication of such stories on deferent electronic platform he underwent enormous pressure and torture and requested the permanent injunction against the defendants. Court vide order dated 19/12/2018 directed the respondent to take down the articles. The High Court acknowledged the right to privacy and held that 'right to be forgotten' and 'right to be left alone' both are inherent part of right to privacy.

[127] Vasunathan v. Registrar General and Ors. W. P. 62038/2016 Karnataka High Court at https://indiakanoon.org
[128] Zulfiquar Ahmen Khan v. M/S Quintillion Business Media Pvt. Ltd. and Ors. C. S. (OS) 642/2018 at https://indiakanoon.org

But this right is not recognised by Information Technology Act, 2000. But it is related to right to privacy and such right is given by Courts.

5.2.2.9 Discussion

Courts in India, provided protection for right to privacy in very limited sense covering few aspects in the beginning. We can observe the evolution as protection to proprietary rights to right to informational privacy and privacy as fundamental right. Protection against search and seizure was provided in M.P. Sarma[129], and Pooranmal,[130] where the right to privacy was tested when the evidence obtained by search breaches the fundamental Right under 20(3). Supreme Court held that Right to Privacy is not available in India as Constitution of India does not provide for it as it is provided under US Constitution. Later it was associated to 'personal liberty and freedom of movement' in Kharak Singh(1963)[131] and Govind[132] (1975), where the court upheld the right to privacy in terms of liberty and freedom of movement without surveillance from government and domiciliary visits in night under the law was held invalid. But Right to Privacy was recognised in minority judgement. It was held that out of other surveillances, surveillance by domiciliary visit was held against the person's right to privacy under Article 21. So the protection was given for personal liberty which is one of the aspects of right to privacy.

The notion that privacy can be compromised by accessing the personal information of the person was considered and recognised much later. Information can be accessed by tapping the telephone. Whether the right to Privacy can be associated with this access. This was discussed in the case of PUCL (1997). Telephone tapping is permissible in India under S. 5(2) of the Telegraph Act, 1885. The writ petition was filed challenging the constitutional validity of the same. The Court held the provision valid but held that tapping should be done for the situations mentioned in Art. 19 (2). For Right to Privacy, the Court held in favour of the contention that telephone conversation in one's

[129] M.P. Sharma v. Satish Chandra, District Magistrate, (1954) SCR 1077.
[130] Pooranmal v. Director of Inspection (Investigation) of Income Tax, new Delhi, AIR 1974, SC 348
[131] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295
[132] Govind v. State of Madhya Pradesh, AIR 1975 SC 1378

home or office is part of the right to Privacy and it is permitted to be tapped under the procedure established by law.[133]

The conflict of two fundamental rights freedom of press and Right to Privacy was discussed in Rajgopal [134](1994). The autobiography of a prisoner-a hard core criminal- was to be published by magazine. It was contended that the published information is infringement of Right to Privacy of prisoner. Publishers challenged the action contending the right to freedom of speech under 19 (1) (a). Supreme Court held that Right to Privacy has achieved the status of fundamental right under Art. 21 but it is not absolute. It is to be decided case by case.

When this right is in conflict with fundamental right of other person, which right will survive? It was answered in the case of Mr. X (1999),[135] where Right to Privacy regarding disclosure of personal information that the person has AIDS was in conflict with the right of his fiancé. It was challenged that disclosure by doctor was against the professional ethics and also breaches the Right to Privacy of Mr. X. Supreme Court held that fundamental right of Right to life is available to his fiancé also. So when Right to Privacy of one person is harming the other person's right to life, in such situations Right to Privacy is not available.

The contention of informational privacy was upheld concretely in Canara Bank (2005)[136], where the provision s. 73 of Stamp Act, which gives power to government to access the documents submitted to any bank for verification of sufficiency of stamp, was challenged. The court held that right to privacy extends to the information in the documents which are submitted to banks as right to privacy protects the persons and not places and persons submitting the documents to the bank have reasonable expectation of privacy. It was held in favour of the petitioner. This case can be termed as 'lamp post' in the privacy judgements in India. But after that, it took long period to decide finally that the informational privacy is an important aspect and is included as a fundamental right under Art. 21 of Constitution of India.

[133] PUCL v. Union of India (1997) 1 SCC 301. P. 311
[134] R. Rajgopal v/s State of Tamilnadu AIR 1994 SCC 632
[135] Mr. X v. Hospital Z, 1999 SC 495, 8 SCC 296
[136] District Registrar and Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496

In the mean while the right was advocated in the cases where information is accessed and published by private entities as newspapers or television serial makers or book writers. The access and publication of such personal information was challenged. The court's stance was not in favour of the persons challenging it on various grounds. This was observed in the following cases. The court had considered the information privacy in some cases e.g. Indu Jain,[137]where information about her achievement of inclusion in Forbus list of billioniars, and Makkal Tholai[138], where the television serial depicting the life of infamous outlaw Veerappan , the right was denied as publishers have right to freedom of expression. But in Phoolan Devi[139], where the film depicting the scenes of gang rape on the famous bandit queen were considered as invasion of right to privacy. In Maneka[140], it was alleged that her Right to Privacy is breached as incidents regarding clashes between Maneka Gandhi and her mother-n-law, Mrs. Indira Gandhi, then Prime Minister of India, were included in the autobiography of Mr. Khushawant Singh, a famous journalist, which he was going to publish. Supreme Court, after considering the material on hand and referring the cases on privacy and other authorities on the right held that fundamental right to privacy is not available to her as publishers are not government. Moreover, personal lives of public figures are always scrutinised by the people and they cannot escape from such scrutiny. Whether they are defamatory, for that purpose she has a right to take action for it in lower court. But there is no right to privacy available in the circumstances.

The Information Technology Act, 2000 was amended to include protection of privacy of person and personal data both. However, the legal challenges brought under the Act have been to decide and fix the liability of the Intermediaries only. A direct case wherein the right to Privacy and provisions of Information Technology Act hasn't come up for consideration before the Courts. However, the cases decided by far are under the provisions were challenging the responsibility of intermediary. Avnish Bajaj[141] was for deciding the

[137] Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006
[138] Makkal Tholai v.Mrs. Muthulakshmi, (2007) 5 M.L.J. 1152
[139] Phoolan Devi v. Shekhar Kapoor and Ors. 57 (1995) DLT 154, (1995) (32) DRJ 142.
[140] Khushwant Singh and Anr. v. Maneka Gandhi, AIR 2002, Delhi 58
[141] Avnish Bajaj v. State (N.C. T) of Delhi. (2005) 3 Comp.LJ.364 Del. 116(2005) DLT 427

responsibility of person publishing the information online and not on the issue of privacy even though selling of obscene material was involved. Shreya Singhal[142] was decided on the issue of breach of fundamental right under Art. 19 (1) (a) speech. Google India Pvt Ltd[143] and Vyakti Vikas Kendra[144] also relating to decision of responsibility of an intermediary.

The decision in Puttaswamy gave conclusiveness to the issue that whether right to privacy-specifically informational privacy- is fundamental right or not. Under e-governance, government delivers services which are done through information technology tools. To decide authenticity of benefit receiver, the government had issued Unique Identification scheme and provided identity cards. For issuance of the card, personal information including biometric information was collected. Separate legislation is enacted for this as Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.[145] This collection of information under Aadhaar Act, 2016 was challenged in K.S. Puttaswamy[146] (2012), on the ground that it is violative of right to privacy.

It was contended by government that Right to Privacy is not guaranteed specifically under Indian Constitution. After verifying legal provisions under different legal systems like USA, UK, European Union, Canada, Russia, South Africa and judgements given by courts in these countries, the Supreme Court unequivocally held the right to privacy is a fundamental right emanated from Art. 21 of Constitution of India. In the judgement it was held by the Supreme Court that where connecting Aadhaar number is not backed by any legislation, demanding Aadhaar number for registration is violative of right to Privacy. On this basis, demanding Aadhaar for mobile connectivity, opening of bank account was held invalid.

The court had verified the data protection under Aadhaar case for the first time and held that there is enough protection mechanism for protection of data collected under Aadhaar Act, 2016 and the Act is constitutionally valid. But

[142] Shreya Singhal v. Union of India, AIR 2015 SC 1523
[143] Google India Pvt. Ltd. v. Visaka Industries Ltd. Crl. P. No. 7207 of 2009
[144] In Vyakti Vikas Kendra v. Jitender Bagga, 2012 AIR (Del) 180
[145] Act 18 of 2016.
[146] J. .K. S. Puttaswamy and Anr. v. Union of India & Ors. W.P. 494 of 2012

some of the provisions were read down or struck down by the Supreme Court as there was a possibility for their misuse or abuse. The government was directed to enact data protection legislation as per recommendation of J. Shrikrishna Committee. On the direction of the court, the government has proposed the Personal Data Protection Bill in 2019.

In all the above cases, Supreme Court was providing protection under Art. 21 Right to Life and liberty of Constitution of India with other laws. The major defence against such right was that the Constitution of India does not provide the right to privacy particularly. And so various aspects of right to privacy were protected by Supreme Court as and when the need arose. From the discussion above, it is also evident that the right to privacy is protected by the court in India as there was and is no legislation for protection of privacy. It has evolved from right to property to personal liberty and slowly extended to privacy of information i.e. data protection.

5.3. Judicial decisions on Right to Privacy and Data Protection in other Countries

The concept 'Privacy' was developed with the growth of civilisation. New aspects of the privacy were emerged after development of various technological innovations. With the growth the information and communication technology, legal systems tried to cope up with the issues emerged. The major threat to an individual is loss of his privacy through breach and invasion. In many cases, the legal framework was developed after these threats were dealt successfully by the judiciary.

The courts in USA had protected right to privacy by interpreting the rights guaranteed under Bill of Rights which are included in Constitution of America as Fundamental Rights. In UK, the protection was provided under the provisions of law of torts, defamation and breach of trust. European Court of Justice has provided the protection against invasion and intrusion of privacy of personal information or data in exemplary way. The Supreme Court of India has provided protection to individuals by interpreting Art. 21 of Constitution of India. But this protection was very inadequate as right to privacy was not recognised specifically and it was totally dependent upon the discretion of the court.

The development of judicial protection for various threats on privacy in different countries under study is discussed in following paragraphs.

5.4 United States of America

In colonial era, the persons accessing the information unauthorised was punished as gossip mongers and eavesdroppers. But they were punished on the grounds of defamation or breach of confidence and not on Right to Privacy. Some rights relating to unauthorised invasion and encroachment by the government were included in Bill of Rights in American Constitution. The Right to Privacy was not provided specifically under the legal provisions including constitutional law. This concept was first time coined by J. Cooley, as 'right to be let alone' in his judgement of 1888 and afterwards fully developed by Warren and Brandeis in their article 'Right to Privacy'[147] in 1890. Courts in America provided protection against invasion on privacy by interpreting the rights and freedoms provided under different provisions of law. It was interpreted by the court that Right to Privacy is covered under the different constitutional amendments also.

5.4.1 Right to search and seizure

The U.S. courts traced and followed the right to privacy as it was followed by the English common law. English Law treated it as a right associated with 'right to property', and was declared that right of privacy is protected by law against trespass to property in **Entick v/s Carrington (1765).** Lord Camden observed: It is an ultimate objective for persons while in society was to secure their property. This right is profound and not communicable in all instances under which it has not been taken away or curtailed by some public law for benefit of whole society. By the laws of England, every invasion of private property, be it even so minute, is trespass. No man can set foot upon the property of the person without seeking permission otherwise he is liable to an action though the damages[148].

[147] Warren and Brandeis, "Right to Privacy", Harvard Law Review, Vol. IV, no.5, 1890
[148] Entick v. Carrington, (1765), EWHC J 98 (KB)

This aspect of privacy as a property right was accepted by US Supreme Court in **Boyd (1886)**[149] and other cases. In that case, the issue was that whether an order for production of invoice for the purchase of 35 cases of glass, which were imported, was violation of right granted against the self- incrimination by Fifth Amendment of Constitution. The court held that it is violation of the right guaranteed by Fifth Amendment and therefore unconstitutional. Other cases followed like **Young (1929)**[150]**,** where defendant has been held liable for intruding plaintiff's home, in **New Comb Hotel Co. (1921)**[151]**,** defendant was held liable for intruding hotel room. This was also followed in **McDaniel(1939).**[152] Supreme Court of Ohio, under the name of privacy –in a case where a creditor hounded the debtor for considerable length of time by telephone calls at his home and his place of employment -held against the defendant.[153]

In the same way, in **Sutherland (1959)**[154] search of plaintiff's shopping bag in a store which she had carried with her when she purchased grocery from the defendant's store was held illegal. Her bags were searched while in presence of other people standing for payment at the counter by the employees on three occasions. The plaintiff was embarrassed and felt nervous. She had to consult a physician. She brought an action for malicious act, slander and right to privacy. The defendant was held liable when the action is brought by plaintiff.

Whether the privacy can be termed as breached when the third party who is in possession of the property or thing owned by the person is searched. In **Miller (1976)**[155] whether the papers of an accused which is in possession of third person if acquired by government without warrant and presented as evidence against him, constitutes breach of rights under Fourth Amendment, was the issue before the court.

[149] Boyd v. United States (1886)116 US 616 (627).
[150] Young v. Western,(1929)
[151] New Comb Hotel Co. v. Corbett 27 Ga.App. 365, 108 S.E. 309 (1921)
[152] McDaniel v. Atlanta Coca-Cola Bottling co.60 Ga. App.92, 2 S.E. 2d 810 (1939)
[153] House v. Peth, 165 Ohio. St. 35, 133 N.E. 2d 340 (1956).
[154] Sutherland v. Kroger and Co;110 S.E. 2d 716 (W. Va. 1959)
[155] U.S v. Miller 425 US 435 (1976)

In this case Miller was arrested for producing liquor illegally in a distillery. During investigation, United States Treasury Department, requested local banks holding Miller's account, to provide all papers of his bank transactions without warrant. Bank complied without giving notice to Miller. These financial records supported the charge which was put on Miller that he had supported with the material and other facilities to run the distillery. At trial at District Court of Georgia, Miller attempted to prevent the submission of bank records as evidence contending that government obtained them without proper subpeona and therefore they are protected from illegal search and seizure under Fourth Amendment. District court rejected the contention and convicted him. Appellate court held in his favour on the basis of the decision in Boyd. [156]

Government filed petition to Supreme Court, questioning whether privacy rights of Fourth Amendment covered the way by which the government obtained the bank record. Justice Powell gave the majority decision and reversed the Appellate court's decision. J. Powell held that "bank records are not private papers of Miller but they are owned by bank as part of its necessary business operations. He stated that there is no expectation of privacy to a customer when he do business through bank. Also checks, deposit slips and other paper work are elements of commercial transaction and they are not private as they are handled by bank employees. There is no intrusion in the area protected by Fourth Amendment". [157]

The age old issue of government's powers regarding search and seizure was challenged in number of cases. The focus was earlier the breach of trespass and other property rights. In **Warden (1967)**[158], Court has recognised right to privacy when issue of illegal search and seizure was challenged on the basis of right to privacy and trespass. In this case, the police was informed about the occurrence of armed robbery and the suspect, the respondent, had entered certain house. After arrival of police at the house, wife of the respondent informed police that she had no objection if they search the premises. Police entered the house and arrested the respondent as they found he was the only man

[156] Boyd v. United States 116 US 616 (1886)
[157] United States v. Miller 425 US 435 (1976) p. 441, 442. www.cdn.loc.gov/service/II/usrep/usrep425/ (Last visited on December 20, 2019)
[158] Warden v. Hayden 387 US 294 (1967).

in the house. Other officers searched first floor and cellar where the arms and ammunition was found.

The search was challenged as it was conducted without warrant but Supreme Court held that, right of the Government to search and seizure has been controlled or regulated by property interests of the person, this presupposition is discredited. It is recognised by the Court that prime objective of Fourth Amendment is the protection of privacy rather than property and the court has discarded fictional and procedural barriers rested on property concepts.[159] The search and seizure was held legal.

After Katz, to determine the breach, the focus was shifted away from approach founded on property rights towards approach based on person's 'expectation of privacy'. But court had not abandoned the rights like right against the trespass totally. This is evident in the following case where Global Positioning System device was used for gathering information. So it can be said that use of modern devices using information technology for obtaining information was tested for breach of person's 'expectation of privacy' in cases 'as search and seizure'.

In **Jones, (2012)**[160] the respondent was suspected for drug trafficking and narcotics violations. FBI installed the Global Positioning System (GPS) under his vehicle for tracking the movements without warrant. This device tracked the movement of vehicle of petitioner 24 hours for four weeks continuously. FBI arrested Jones and court convicted him for distributing and possessing with intent to distribute the narcotic drugs. In appeal, Jones argued that his conviction should be overturned as installing GPS device without warrant was 'search' breaching his rights under the Fourth Amendment. United States Court of Appeal for Columbia District overturned Jones conviction holding that GPS monitoring was search under Fourth Amendment breaching his right for "reasonable expectation of privacy".

In petition to Supreme Court, the court had to decide the questions 1) Whether the use of tracking device without obtaining a warrant for monitoring the movements of respondent violated Fourth Amendment, 2) whether the

[159] Warden v. Hayden 387 US 294 (304) (1967)
[160] United States v. Jones 565 US 400 (2012)

respondent's Fourth Amendment rights are violated by installing the GPS tracking device on his vehicle without valid warrant and without his consent by government.

Nine judges unanimously held in favour of Jones holding that the installation of device is 'search' under Fourth Amendment. Justice Scalia, for majority held that, " 'search' covered under Fourth Amendment is "rights of the people to be secure in their person, homes, papers, and effects, against unreasonable searches and seizures, shall not be violated". Court cited the case US v. Chadwick 433 U. S. 1, 12 (1977) and held that vehicle is an "effect" as the term used in amendment. So government's use of tracking device is 'search'."[161] He held that a trespass test under Fourth Amendment need not exclude a test of expectation of privacy, which may be appropriate to consider in situation where there was no government trespass. [162] The Court held that installing GPS device to the vehicle of Jones without his consent is trespass and search.

Whether obtaining information from service providers of mobile connection amounts to 'search' by the police? This question was under scrutiny in **Carpenter's[163]** case. The issue was relating to mobile communication data – cell-site location information (CSLI) of the petitioner, which was accessed by FBI for investigation of robbery cases. The FBI had arrested four persons for robberies. One of them confessed the crime and provided his cell phone and also cell phone numbers of other men. The FBI acquired the call records from the mobile service providers and accordingly charged the petitioner. Petitioner challenged the action of the state that his call records are the personal data which was accessed without warrant, therefore his rights against unreasonable search and seizures under Fourth Amendment were violated. The District court and Court of appeal denied the motion holding that Carpenter lacked 'reasonable expectation of privacy' and access to call records was not 'search'.

Carpenter appealed in Supreme Court, which had considered the various referred cases including Katz. It was held by the majority that, cell phone

[161] United States v. Jones 565 US 400 (2012), (Slip opinion) p.3, at www.courtlistener.com/pdf (Last visited on December 20, 2019)
[162] United States v. Jones, 565 US 400 (2012) (Slip Opinion), p.5, 11. www.supremecourt.gov/opinions (Last visited on December 20, 2019)
[163] Carpenter v. United States 585_US (2018).

location information is automatically gathered in detailed, encyclopaedic and effortless way and compiled once he is registered with the service provider. By this, individual continuously reveals his location. Cell phone records are unique in nature in this way.[164] Government gains the advantage of the technology of wireless carrier. This location information, provides all-encompassing record of whereabouts of holder. The time-stamped data provides all information including personal and intimate information also and reveals not only his particular movements but through them his "familial, political, professional, religious and sexual associations" are also known."[165] The Court held that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. And therefore the location information obtained from carpenter's wireless carriers was the product of search. [166] And it was held as breach of the rights under Fourth Amendment.

But still it was very difficult to get success if action was brought under the claim of privacy right only and no other ground was contended. This is seen in the case of B**oring.** [167] Boring sued Google for invasion of privacy and trespass after Google's Street View car drove down their private road and captured Boring's house and pool on its camera, which was displayed in Google's Street View feature. Dismissing Boring's claim of intrusion upon seclusion and publicity given to private life, court found no reasonable person would find a car driving down a driveway and taking picture "highly offensive", pointing out that salespersons or delivery persons would make the same trip, and also picture did not display the Borings.

However 3rd Circuit Court reversed the District court on trespass claim and allowed the action as physical trespass is a strict liability tort and complaint did allege that Google's car entered on to Boring's private land. So the he succeeded on the ground of trespass and not on the ground of breach of privacy right.

[164] Carpenter v. United States 585_US (2018) (Slip Opinion) p. 10, 11. www.supremecourt.gov/opinions (Last visited on December 20, 2019)
[165] Carpenter v. United States 585_US (2018)(Slip Opinion) p. 12, www.supremecourt.gov/opinions (Last visited on December 20, 2019)
[166] Carpenter v. United State 585_US (2018) (Slip Opinion) p.11, www.supremecourt.gov/opinions (Last visited on December 20, 2019)
[167] Boring v. Google Inc. No. 09-2350, 2010. US App. LEXIS 1891 (3rd Cir. Jan 25, 2010)

5.4.2 Right to Personal liberty

Another aspect of privacy is liberty to take decisions for oneself relating to marital relationship. It came for consideration in case for the use of contraceptive by any person. The law banning the use of any medical device, drug for contraception by State of Connecticut was in question. In **Tileston v. Ullman (1943)[168],** a doctor challenged this law. There was a ban on contraception. Therefore he wanted a declaratory judgement that such law is against the Fourteenth Amendment of the Constitution. Supreme Court dismissed the plea on the ground that Plaintiff lack standing to sue on behalf of patients. They were not the parties in this action. There was no allegation that the plaintiff's life in danger.

But in **Poe v. Ullman (1961)[169]**, Paul and Poe, a married couple decided to use contraceptive to prevent fourth pregnancy after their first three children died in infancy. Another woman, Jane Doe, wanted to access contraceptive to prevent second pregnancy which could be life threatening. Connecticut law was banning the use of contraceptive. Both of them challenged the law that it is against the Fourteenth Amendment and therefore unconstitutional. But the law was not enforced against them and they were not charged still they were challenging the Law. This fact went against them.

Supreme Court dismissed it as plaintiffs had not been charged or threatened with prosecution so there is no controversy to be resolved by the court. Frankfurtur J held that without suffering any hardship, on apprehension of mere existence of penal statute is not sufficient grounds to challenge its constitutionality.[170]

When the right to personal privacy came up for consideration in **Griswold (1965)**[171], in the absence of specific provision in US Constitution, the Court traced the emergence of right to privacy from the right to freedom of expression and other rights. In this case, Connecticut Act was challenged. The Act made it illegal to use of any drug, medicinal article, or instrument for the purpose of preventing contraception. To help the contraception in married couples, Planned

[168] Tileston v. Ullman, 318 U S 44 (1943)
[169] Poe v. Ullman, 367,U S 497 (1961)
[170] Poe v. Ullman, 367,U S 497 (1961) Pp. 507, 509.
[171] Griswold v. State of Connecticut 381 US 479 (1965)

Parenthood clinics were established in the State and they were compelled to follow this law. Appellant Griswold was Executive Director of Planned Parenthood League of Connecticut and Appellant Buxton is licenced physician and Professor at Yale Medical College. They were arrested for breaking the law. It was challenged that this law is unconstitutional as it violates the rights guaranteed under Fourteenth Amendment. They were held guilty. The appellate court and State High court affirmed the judgement.

The Supreme Court, after referring the cases cited by the parties, held that, specific guarantees in Bill of Rights have penumbras. Various guarantees create zones of privacy. To give them life and substance the penumbras of these rights in Bill of Rights help. Court observed that in present case, relationship covered in the zone of privacy is created by several fundamental constitutional guarantees. And law is forbidding the use of contraceptives to achieve its goal, rather than regulating their manufacture or sale. This forbidding the use of contraceptive has more destructive impact upon relationship. Court held that such a law cannot be validated on principles which are often followed by the court. The government's purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which provide broad powers and thereby invade the area of protected freedoms. [172] The law was held unconstitutional.

In Griswold, freedom to decide for one's personal life relating to family life was recognised. But it was recognised for married persons. The right to use contraceptive by unmarried person was not recognised. The question was discussed in the following case. In **Eisenstadt v. Baird (1972)[173],** equality regarding Right to Privacy for using contraceptive measures by the unmarried couples are achieved. In this case, the appellant was convicted on violating a Massachusetts law for giving contraceptive foam to students at the end of the lectures on contraception. The Massachusetts law prohibits to give any drug, medicine, instrument or article for prevention of conception except on the basis of registered physician's prescription to married person. He was charged on two grounds, one giving lectures on contraception though he is not registered

[172] Griswold v. State of Connecticut 381 US 479 (1965) Pp. 484, 485.
[173] Eisenstadt v. Baird, 405 U S 438(1972).

pharmacist and secondly, giving contraceptive foam to a woman. He challenged his conviction. District Court dismissed his petition. Appellate court vacated the dismissal but held him guilty for providing contraceptive foam to a woman and remanded the case. The ruling was then appealed.

The Supreme Court, held the Act unconstitutional. Confirming the Appellate court's opinion, J. Brennan held that Court of Appeal concluded that the statutory goal as to limit contraception in and of itself- a purpose that the court held conflicted "with fundamental human rights" under Griswold, where the court struck down Connecticut's prohibition against the use of contraceptives as an unconstitutional infringement of the right to marital privacy. The court also agreed that goals of deterring premarital sex and regulating the distribution of potentially harmful articles cannot reasonably be regarded as legislative aims of the Act. So it was held that the statute, violates the rights of single persons under Equal Protection Clause of Fourteenth Amendment.[174]

The leading case regarding extension of the right of parenting is **Roe (1973)**[175]. Appellant Jane Roe was pregnant and wanted to abort. The Texas statute provided the abortion illegal except the life of mother is in danger. She submitted that she is unmarried and pregnant and she could not get help of physician to abort as her life is not endangered as per the statute. She has challenged the statute as unconstitutional breaching the personal liberty guaranteed under Fourteenth Amendment. Court held that the right to privacy, whether it is founded in Fourteenth Amendment's concept of personal liberty and restriction upon state actions, is broad enough to encompass a women's decision whether or not to terminate her pregnancy. Therefore court concluded that right of personal privacy includes the abortion decision but it is not absolute and must be considered against important state interests in regulation.[176]

After considering the facts and legal principles involved in the case, Court struck down Texas Law that criminalise aiding a woman in getting an abortion. It was held that a state criminal abortion statute of the current Texas type, that except from criminality only a life-saving procedure on behalf of a mother without

[174] Eisenstadt v. Baird, 405 U S 438(1972) P. 442,443
[175]Roe v. Wade 410 US 113 (1973).
[176] Roe v. Wade 410 US 113 (1973) P.153

regard to pregnancy stage and without recognition of other interests involved is violative of Due Process Clause of Fourteenth Amendment."[177]

5.4.3 Right to Privacy of Personal Communication

The right to privacy was associated to the property interests earlier. With progressing time, the focus of right to Privacy is broadened as privacy of home or property shifted to 'expectation of privacy' at places outside home also. This term is used in Katz case as 'privacy reason'. In **Katz (1976)**[178]**,** petitioner, was convicted under the charges of transmitting wagering information in college basketball through public telephones. It was an offence under gambling law in US. Federal Bureau of Investigation (FBI) officers recorded these conversations by using covert listening devices attached to public phone booth near his apartment. He was arrested and the recording was presented as evidence in the court. Katz challenged this as it is violation of his rights under Fourth Amendment and contended that the recording should not be used as evidence as FBI had not taken warrant for collecting it.

The majority 7-1, opinion delivered by Justice Stewart, laid down that the "Fourth Amendment protected 'people and not places' and Fourth Amendment governs not only the seizure of tangible items, but extends as well to recording of oral statements, overheard without any "technical trespass" under local property law. Silverman v. United States, 365 US 505, 511."[179] Court concluded that government's activities in electronic listening to recording the petitioner's words violated the privacy upon which he justifiably relied while using telephone booth and thus constituted 'Search and seizure' within the meaning of Fourth Amendment.[180]

Harlan, J. in his concurring opinion said that the scrutiny under Fourth Amendment would be done whenever official investigative activity invaded 'a reasonable expectation of privacy'.[181] He observed that two things are necessary

[177] Roe v. Wade 410 US 113 (1973) P. 164
[178] Katz v. United States 389 US 347 (1976). www.cdn.loc.gov/service/II/usrep389 (Last visited on December 17, 2019)
[179] Katz v. United States, 389 US 347 (!976) P. 353 www.cdn.loc.gov/service/II/usrep389 (Last visited on December 17, 2019)
[180] Katz v. United States, 389 US 347 (!976) P. 353 www.cdn.loc.gov/service/II/usrep389 (Last visited on December 17, 2019)
[181] Katz v. United States 389 US 347 (1976) p. 360 www.cdn.loc.gov/service/II/usrep389

to formulate 'reasonable expectation' – a) Person has exhibited an actual (subjective) expectation of privacy and b) expectation should be one as 'reasonable' as recognised by the society. A person's home, for most purposes, is a place where he expects privacy, but his objects, activities or statements that he exposes to outsiders are not protected as his intention to keep them to himself is not exhibited. But conversation in open world would not protected against being overheard, because the expectation of privacy under the circumstances would be unreasonable.[182] Harlan J. held that when petitioner uses telephone in public booth, he shuts the door of the booth. By this he shows his intention to keep the matter to himself and he does not want to expose them to others. So first test is proved. [183] So everything depends upon the behaviour of the person. The second test is proved, when such expectation is 'reasonable' according to the standards prevailed in the society.

Although the phrase came from Justice Harlan's separate opinion, it is treated today as the essence of the majority opinion. The test gives more flexibility to protect broader concept of human dignity at a time when information technology had overshadowed what property rights alone could protect.

In Katz the protection was provided against the State. But if the private party invades the privacy of communication, whether the protection is available. In **Fischer (2002)[184]** defendant-employers monitoring of Plaintiff-employee's telephone conversation and accessing plaintiff's web based e-mail account. Court held that the case is covered under Electronic Storage Communication Act as defendant hired a computer expert and guessed plaintiff's password so as to access and review plaintiff's web based e-mails. Defendant was also held liable under Wire Trap Act and it was also held that defendants should have ceased to listen to conversation when they discovered it was personal in nature.[185]

[182] Katz v. United States, 389 US 347 (!976) P. 361 www.cdn.loc.gov/service/II/usrep389 (Last visited on December 17, 2019)
[183] Katz v. United States, 389 US 347 (1976) p. 361, www.cdn.loc.gov/service/II/usrep389 (Last visited on December 17, 2019)
[184] Fischer v. Mt. Olive Lutheran Church Inc. 207 F. sup. 2d 914. (W. D. Wis. 2002).
[185] Fischer v. Mt. Olive Lutheran Church Inc. 207 F. sup. 2d 914. (W. D. Wis. 2002) p. 923.

5.4.4 Right to Disclosure of Information.

As mass media like television was advanced, intrusion in personal life is increased and norms of privacy have also changed. Sometime the intrusion become voyeuristic in nature. Such intrusion many times involved threats regarding reputation, liberty and freedom of decision making. **William Prosser**[186] put forward the concept of tort of privacy with regard to this intrusive mass media, first by newspapers then by television, by highlighting four types of torts inclusive of other torts.

1. He explained the first tort- "intrusion upon a person's solitude-where he explained that intrusion must be offensive or objectionable for reasonable man"[187]. In a public street a man has no right to be let alone, but in his home or placed where he generally expect that he has right to be in seclusion, intrusion in such areas is objectionable.

2. His second tort is public disclosure of embarrassing facts of person's private life. There will be liability only for publicity given to those things which the customs and ordinary views of the community will not tolerate. This is distinct from intrusion. This interest protected is that of reputation with some connotations of mental distress that are present in libel and slander. It is really an extension of defamation. Here the facts must be private and they are made public.

He referred the case of **Sidis (1938)**[188]**,** where William James Sidis was a child prodigy. He graduated from Harvard at the age of 16. At the age of 11 years, he lectured to eminent mathematicians on 4th dimension. When he arrived at adolescence, he developed some psychological changes, due to which he shunned publicity. He disappeared, led unknown life as book keeper and occupied himself in collecting street car transfers and other things. The New Yorker Magazine found him and published sympathetic story of his career, revealing his present whereabouts and activities. He challenged the publication inter alia on breach of his right to privacy.

[186] Prosser, William, 'Privacy', 48 California Law Review, 383, 388-389 (1960)
[187] Prosser, William, 'Privacy', 48 California Law Review, 383, 388-389 (1960)
[188] Sidis v. F.R. Publishing Corporation 113 F 2d 806 (2d Cir. 1940); affirming 34 F Supp. 19 (S.D.N. Y.1938)

Court took into consideration the article written by Warren and Brandies and held that even though there are contrary opinions for granting immunity against disclosure for protection personal information it is not possible to grant absolute immunity to all of the personal details of personal life from the press. The public interest in obtaining information becomes dominant over individual's desire for privacy at many times. The court held that limited scrutiny of 'private' life of any person who has achieved or has had thrust upon him, status of 'public figure,' is permitted to satisfy the curiosity of public.[189]Effect on Sidis was devastating and resulted to his untimely early death. But outcome of the story suggests that intrusion can be destructive.

3. Prosser explained the third tort as-"publicity which places an individual in false light in public eyes. He gave an example of Lord Byron- who, in 1816, succeeded in enjoining the circulation of spurious and inferior poem attributed to his pen.[190] Publicity falsely attributed to Plaintiff some opinion or utterance. He further described another form of this type – i.e use of Plaintiff's picture to illustrate a book or an article in which he has no reasonable connection.

In public interest it is somewhat agreeable but where a face of some innocent and unrelated citizen is employed to decorate an article on 'Negligence of children' as in **Leverton (1951)**[191] or peddling of narcotics as in **Thompson**.**(1950)**[192] there is an obvious innuendo that article applies to him, which places him in a false light before the public and is actionable.

4. The fourth tort is explained by Prosser is "Appropriation to a person's advantage of another's name or likeness.[193] He explained this with the help of cases, **Macanzie (1891)**[194] and **Kerby (1942)**[195] Name of the plaintiff has been used without his consent to advertise defendant's product. Anybody can take name of any great and famous person but when he uses it for some advantage of his own, he becomes liable. It is in this sense that 'appropriation' is to be

[189] Sidis v. F.R. Publishing Corporation 113 F 2d 806 (2d Cir. 1940), p. 809.
[190] Lord Byron v. Johnson, 2 Mer. 29, 35 Eng. Rep. 851 (1816)
[191] Leverton v. Curtis Publishing Co 192 F 2d 974 (3rd Cir. 1951)
[192] Thompson v. Close-up, Inc 277 App. Div. 848, 98 N.Y.S. 2d 300 (1950)
[193] Prosser W., 1960, 'Privacy', California Law Review, 48: 383-423.
[194] Macanzie v. Soden Minaral Springs Co.27 Abb. N. Cas. 402, 18 N.Y.S. 240 (Sup.ct. 1891)
[195] Kerby v. Hall Roach Studios 53 Cal. App. 2d 207, 127 P. 2d. 577 (1942)

understood. If this name can be identified with the name of plaintiff then Plaintiff is entitled to the protection against its use. There is no liability for using hand, foot or dog of famous person if nothing is there to indicate to whom they belong. He explained that privacy tort applied only when an identified person was involved.

The recognition of this fourth tort is found, though it was propounded much later in time, in the case of **Rochester Folding Box Co**. **(1902)**[196], wherein the defendants made, printed, sold and circulated about 25,000 lithographic pictures resembling the plaintiff without her consent for advertisement. These pictures were published for advertising the flour which the Frankline flour company was producing. Those photographs were pasted in stores and other public places all over United States including in the vicinity of the residence of plaintiff. The Plaintiff claimed that because of this, she has suffered severe nervous shock and compelled to consult a physician. She also contended that her reputation is attacked, causing her distress and suffering both in body and mind. She had submitted that the defendants shall be restrained from making, printing, publishing or circulating in any manner her picture, resemblance, photograph of the plaintiff and damages shall be awarded to her.

The trial court issued the interlocutory judgement in favour of plaintiff. But it was overruled in appeal. The court held in four-to-three decision that the right to privacy did not exist as there is lack of precedent[197]. Justice Gray, (minority opinion) vigorously argued for the active protection of the right of privacy. The American Courts considered the views of Warren and Brandeis on privacy for the first time in 1902 in this case.

But it took three more years for courts to recognise the Right to Privacy. In **Pavesich (1905),**[198] for the first time the right of privacy was recognised and enforced by the American Courts. In that case, Defendant's insurance company used Plaintiff's name and picture, as well as bogus testimonial from him in advertisement. Georgia court accepted views of Warren and Brandeis and recognised the existence of distinct right of privacy. For next thirty years, there

[196] Roberson v. Rochester Folding Box Co. (1902), 171 N.Y. 536.
[197] Roberson v. Rochester Folding Box Co. (1902), 171 N.Y. 536.p. 544
[198] Pavesich v. New England Life Insurance Co (1905), 122 G.H. 190.

was a continued dispute as to whether the right of privacy existed at all as courts elected to follow Roberson or Pavesich.

In America during 1960, computers were permitted in public offices and private companies. Data generation and data gathering is increased. It has become easy to search the information of any person by linking various other information about him by way of processing. By technology, non-identifiable data can be turned into identifiable data which can be linkable to individual. Intrusion and publicity of such personal facts through electronic media is more harmful as it gives wider publicity. Liberty and freedom and privacy of individual is now more at risk.

The most common violation of privacy is publishing the information by press in electronic media. In **Shulman (1998)**[199], Ruth Shulman and one of her family members were injured while travelling when their car skidded on the highway and was overturned. They were trapped in the car. A medical team gave assistance to them. While carried by the paramedics, one news reporter, who was working with Group W. Productions filmed their extraction and also recorded their audio conversation with nurse. After editing, the video and audio were broadcasted on T.V. documentary show. Neither Shulman nor her family member was consented for publication. They sued for invasion of privacy.

California Law provides for the liability of the person in tort, who intentionally intrudes upon a private place, conversation or matter of another in a manner that is highly offensive to a reasonable person. The dispute was regarding the right to privacy of an individual under Fourteenth Amendment and freedom of expression (press) guaranteed under First Amendment. It was held that unauthorised collection of data in video and audio of conversation with nurse for newsgathering is an intrusion into another's seclusion[200].

With the use of Internet of Things (IoT), devices are connected to each other and with use of technique of Artificial Intelligence, many tasks are performed. Because of this, possibility of gathering information in the electronic devices is increased. The corporation providing these services uses the collected

[199] Shulman v. Group W. Productions Inc.18 Cal. 4th 200 (1998).
[200] Shulman v. Group W. Productions Inc.18 Cal. 4th 200 (1998).

information for commercial purposes. The privacy of person is compromised by commercial use of their personal information. Legal systems try to provide protection under Data Protection legislation but it is very difficult because of intricacies of technology and failure of the individuals in visualising the all possible effects on their privacy in future.

5.4.5 Right to Protection of Data

But while using electronic media via internet, the browsing activities are recorded with the service provider and also can be gathered through cookies. When any application is facilitating the use of internet for betterment of services, the personal information is collected and deposited, and used for some commercial purpose. Whether it is a right of the person who is using the application, that his information shall not be used without informing him about purpose of use. The issue was raised in **Supnick,(2000)**[201] where, in class action suit against Amazon and Alexa, alleged that Alexa whose software programme monitors surfing habits and then suggests related web pages, stored and transmitted this information to third parties including Amazon without informing users of the practice or obtaining user's consent[202]. The law suit came after a privacy complaint filed with Federal Trade Commission by computer security expert Richard Smith. Smith alleged that company is gathering more private information than Amazon acknowledges. Plaintiff claimed these practices violated Electronic Communication Protection Act (ECPA) and constituted a common law invasion of privacy[203]. Court approved settlement agreement. The terms required Alexa to a) delete four digit in IP addresses in its data bases, b) add privacy policy information to its website, c) require customers to opt in to having their data collected before they are permitted to download Alexa software and d) pay-up to $40 to each customer whose data was found in Alexa's data base.[204]

It is very difficult for common person to prove the misuse of information by such corporations who are service providers. Moreover it is not always possible

[201] Supnick v. Amazon.com, Inc; 2000 US District LEXIS 7013 (W.D. Wash.2000).
[202] Supnick v. Amazon.com, Inc; C00-022IP, p.7(W. D. Wash. June 20, 2000) (complaint)
[203] Supnick v. Amazon.com, Inc; C00-022IP, p.7(W. D. Wash. June 20, 2000) (complaint)
[204] Supnick v. Amazon.com, Inc; C00-022IP, p. 7(W. D. Wash. June 20, 2000) (settlement agreement dt. April 16 and final order and judgement on July 27, 2001)

to implement existing provisions to the threats by innovative uses of technology. The protection provided to such cases are very difficult to obtain.

5.4.6 Discussion

From the above discussion, it can be observed that right to privacy as a concept is developed with the development of the society. From the beginning the concept was associated to the physical belonging of an individual, all of them were material things. The concept was extended when feelings, emotions, spiritual nature of an individual were also included as important elements for the protection of privacy. It was acknowledged first by courts by interpreting the existing provisions of law including provisions in Bill of Right relating to amendments to the Constitution. The concept privacy has evolved from the privacy of person relating to property in Boyd (1886)[205] which was followed in New Comb Hotel (1921)[206], intrusion in hotel room. The power of search and seizure of not only the government but private entities were challenged in Sutherland (1959)[207] where search of shopping bag by owner was held that it is a breach of privacy. This protection against the power of search was extended when search was conducted using Global Positioning System in Jones (2012)[208], it was held illegal as conducted without obtaining the consent of the owner. The same protection was provided when mobile data was accessed and collected by the mobile service provider by police in Carpenter (2018)[209].

The protection relating to personal liberty especially to matters pertaining to family and procreation was provided in Tilston (1943)[210], Poe (1961)[211] and Griswold (1965)[212] for choosing contraception by married couple. Court held that individual is free to take any decision relating to his family and personal life and legislation invalidating such decision was held unconstitutional. Same way the protection for decision of abortion in Roe (1973)[213] was given. Decision

[205] Boyd v. United States (1886)116 US 616 (627)
[206] New Comb Hotel Co. v. Corbett 27 Ga.App. 365, 108 S.E. 309 (1921)
[207] Sutherland v. Kroger and Co;110 S.E. 2d 716 (W. Va. 1959)
[208]United States v. Jones, 565 US 400 (2012)
[209] Carpenter v. United State 585_US (2018)
[210] Tileston v. Ullman, 318 U S 44 (1943)
[211] Poe v. Ullman, 367,U S 497 (1961)
[212] Griswold v. State of Connecticut 381 US 479 (1965)
[213] Roe v. Wade 410 US 113 (1973).

for using contraceptives by unmarried person was upheld on the ground of equality in Eisenstadt (1972)[214].

Yet another aspect relating to privacy i.e. privacy of communication was protected under Katz (1976)[215], where tapping of the telephone was held as breach of right to privacy by enlarging the concept by 'reasonable expectation of privacy' and in Fischer (2002)[216] where accessing the information from the emails of employees was held as breach. As provisions relating to protection from the disclosure of information by media-print as well as electronic- was provided in Rochester Folding Box Co.(1902[217]) and Paveseich (1905)[218]where the information was used in advertisement without consent of the person. The disclosure by electronic media was held as breach of privacy in Schulman (1998)[219] when details of the accident was shown in television show. The privacy of the personal data was protected in Supnic(2000)[220] when personal data provide to Alexa app was used by Amazon for commercial profit, it was held that it is breach of privacy of personal information.

From the discussion of all the above cases it can be experiential that as there was progress in technology, the protection of privacy was extended by expanding the definition of 'privacy' encompassing the new avenues of personality of an individual from personal liberty to protection of data. The concept of privacy was expanded to include the technological advancements; like the notion of search and seizure was extended from physical search to planting of GPS in vehicle. The cases dealt with above underline the point that the informational privacy and data protection are inevitable facets of right to privacy.

5.5 United Kingdom

British constitution is in unwritten form. In Britain there are no specific provisions for right to privacy under the constitution as a fundamental right. In

[214] Eisenstadt v. Baird, 405 U S 438(1972)
[215] Katz v. United States, 389 US 347 (!976)
[216] Fischer v. Mt. Olive Lutheran Church Inc. 207 F. sup. 2d 914. (W. D. Wis. 2002) p. 923.
[217] Roberson v. Rochester Folding Box Co. (1902), 171 N.Y. 536.p. 544
[218] Pavesich v. New England Life Insurance Co (1905), 122 G.H. 190.
[219] Shulman v. Group W. Productions Inc.18 Cal. 4th 200 (1998)
[220] Supnick v. Amazon.com, Inc; C00-022IP, p. 7(W. D. Wash. June 20, 2000) (settlement agreement dt. April 16 and final order and judgement on July 27, 2001)

the beginning, the right to privacy was protected up to certain extent under Law of Torts, provisions of defamation and of trespass to property or person. But Law of defamation does not provide any protection where the facts are true. He had to argue on the basis of breach of confidence if the relationship is of formal nature. As under other legal systems, Court protected the right of the person as right relating to property. The court at times also held that the person had property interest in the letters he has written to others. The Courts provided protection for the right in name of breach of person's reputation if information is disclosed or on the basis of breach of confidence. The researcher has discussed the development from right relating to property to right to protection of data in following paragraphs.

5.5.1 Right to search and seizure

Right to privacy starts in English law with the concept of his right to enjoy the property. The Right to Privacy and the power of the State to interfere-by search, seizure, interception in any way- have been the debate in almost every democratic country where fundamental freedoms are guaranteed. This takes us back to the case of Semayne decided in 1603 (5 Coke's Rep. 91a) (77 Eng. Rep.) where it was laid down that 'Every man's house is his castle'. But no general right to privacy was existed in England. Partial protection is existed through tort remedies like trespass, defamation and breach of confidence. The law of confidence prevents other party to disclose the information about the person. In **Pope (1741),**[221] Curl published five volumes of Pope's private letters, including the twenty seven years of history of correspondence with Jonathan Swift. Pope challenged him. The injunction was granted. Curl filed an action to vacate the injunction. It was held that the collection of letters and other books are within the meaning of the statute made in 8th year of Queen Anne, C.19, An Act meant for encouragement of learning. Lord Hardwick observed that, "It is only a special property in the receiver, possibly property of the paper may belong to him, but this does not give licence to any person whatever to publish them, to the world, for at most the receiver has only a joint property the writer."[222]

[221] Pope v. Curl (1741),26,Eng. Rep. 608(A), t www.commonlii.org/uk/cases (Last visited on December 17, 2019)
[222] Pope v. Curl (1741), 26 Eng. Rep. 608 (A), p. 608 at www.commonlii.org/uk/cases (Last visited on December 17, 2019)

Injunction was continued only as to those letters "which are under Mr. Pepe's name in the book and written by him, not as to those which are written to him."[223] Court found it difficult to punish him in copyright law therefore protected him in right to privacy in correspondence. The court recognised that there was a value in personal communication.

In a landmark judgement in **Entick (1765)**[224], the king's messengers broke into the house of writer Entick and searched his house for writings. They broke opened the locked door, cabinets, drawers. Search was ordered by Secretary of State. The defendant's claimed that they had acted on the warrant issued by Secretary of State and therefore are not liable. Lord Camden held that secretary of State had no authority under statute or by precedent to issue warrant and therefore search was illegal. Lord Camden declared the behaviour as subversive 'of all the comforts of society' and held "The great end, for which men entered into society, was to secure their property. That right is preserved sacred and incommunicable in all instances, where it has not been taken away or abridged by some public law for the good of the whole. The cases where this right of property is set aside by private law, are various. Distresses, executions, forfeitures, taxes etc. are all of this description; wherein every man by common consent gives up that right, for the sake of justice and the general good. By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my licence, but he is liable to an action, though the damage be nothing; which is proved by every declaration in trespass, where the defendant is called upon to answer for bruising the grass and even treading upon the soil. If he admits the fact, he is bound to show by way of justification, that some positive law has empowered or excused him. The justification is submitted to the judges, who are to look into the books; and if such a justification can be maintained by the text of the statute law, or by the principles of common law. If no excuse can be found or produced, the silence

[223] Pope v. Curl (1741), 26 Eng. Rep. 608 (A) p.608 at www.commonlii.org/uk/cases (Last visited on December 17, 2019)

[224] Entick v. Carrington (1765) (19 Howells' State Trials 1029) (95 Eng. Rep. 807) at www.bailii.org/ew/cases/EWHC/KB/1765/J98.html (Last visited on December 17, 2019)

of the books is an authority against the defendant, and the plaintiff must have judgment."[225]

In earlier cases, breach of privacy was challenged on basis of breach of various other rights as right to privacy was not provided for. Therefore though right involved was privacy of personal letters, sketches or correspondence, the cases were decided on the breach of property in trespass or breach of confidence than right to privacy.

Some of the cases which were decided applying these rights are as follows. The first one is **Gee (1818)**[226] which held that the person has property rights in the letters written**.** In this case Mr. Gee was a landlord and Mr. Pritchard was a son of his. Mrs. Gee was stepmother of Mr. Pritchard, who used to write letters to him when they were on good terms. After some years, their relations were strained and Mrs. Gee stopped writing to Pritchard. He wanted to publish these letters. Action was brought by Mrs. Gee against her step son, Rev, Pritchard, who had tried to publish his private correspondence with her on the ground that the material would wound her feelings. Lord Eldon held "case could proceed on fact of property but not on the idea of feelings, or wounded feelings or violation trust or pledge."[227] It was held that "Plaintiff has sufficient property in original letters to authorise in an injunction."[228] Court issued injunction order preventing publication as Mrs. Gee has property rights in letters.

But in many cases court found it appropriate to decide the case on the basis of breach of confidence. In **Strange, (1848)**[229] Queen Victoria and Prince Albert had created various etching as hobby. These etchings were given to take prints to Mr. Brown. Good copies and plates of etchings were returned by Mr. Brown. But some extra copies were sold by the employee of Mr. Brown. These copies

[225] Entick v. Carrington (1765) (19 Howells' State Trials 1029) (95 Eng. Rep. 807) at www.bailii.org/ew/cases/EWHC/KB/1765/J98.html (Last visited on December 17, 2019)

[226] Gee v. Pritchard 36,Eng. Rep. 670 (1818), at www.commonlii.org/uk/cases/EngR/1818/605.pdf (Last visited on December 17, 2019)

[227] Gee v. Pritchard, 36 Eng. Rep. 670 (1818) p. 677, at www.commonlii.org/uk/cases/EngR/1818/605.pdf (Last visited on December 17, 2019)

[228] Gee v. Pritchard, 36 Eng. Rep. 670 (1818) p.678, at www.commonlii.org/uk/cases/EngR/1818/605.pdf (Last visited on December 17, 2019)

[229] Albert v. Strange, 41 Eng. Rep. 1171 (Ch) (1848), at www.commonlii.org/uk/cases/EngR/1849/255.pdf (Last visited on December 17, 2019)

were used by writer Judge, who published the book in 1848, 'Sketches of Her Majesty's Household'. Mr. Strange, a publisher of the book tried to exhibit the etching done by Queen Victoria without the Royal permission. Prince Albert challenged and wanted to seek injunction for this exhibition, surrender of the copies of etchings etc.

Lord Chancellor raised a question that "how far this publication is violation of law? That there is a property in ideas which pass in the man's mind is consistent with all the authorities of English law. Incidental to that right is right of deciding when and how they shall be made known to public. Privacy is part, an essential part of this species of property."[230] The court was going to rule in favour of Royal family even in absence of clear statute that protect it. "In the present case, where privacy is the right invaded, postponing the injunction would be equivalent to denying it." [231] He said.

The right to privacy was in question even in cases of prisoners, where cells of prisoners were searched in absence of them in **R (Daly) (2001)**[232]. It was observed that even when regular search was conducted in past, large quantity of objectionable material-drugs etc. was found from the cells of prisoners. In 1995, the Home Secretary introduced a new policy governing the searching of the cells occupied by convicted and remand prisoners' in closed prisons in England and Wales. Under this policy, the instructions for the prison governors were given about powers of extensive and thorough search of the prison cell shall be conducted by them. During the search, the prisoner shall not be present. It is provided that during the cell search, staff must examine legal correspondence thoroughly in absence of the prisoner. It must be examined only so far as necessary to ensure that it is bona fide correspondence between the prisoner and his legal advisor and does not conceal anything else.

Dally challenges the lawfulness of policy as it makes mandatory the absence of prisoner when his cell is thoroughly searched including his legal

[230] Albert v. Strange, 41 Eng. Rep. 1171 (Ch) (1848) p.1307 at www.commonlii.org/uk/cases/EngR/1849/255.pdf (Last visited on December 17, 2019)
[231] Albert v. Strange, 41 Eng. Rep. 1171 (Ch) (1848)p.1312, at www.commonlii.org/uk/cases/EngR/1849/255.pdf (Last visited on December 17, 2019)
[232] R (Daly) v. Secretary of State for Home Department (2001) 2 AC 532 at https://publications.parliament.uk/ (Last visited on December 10, 2019)

correspondence. He contended that legal correspondence is privileged communication and this blanket policy infringes his right regarding correspondence, recognised under common law and under European Convention of Human Right protection.

The court held that "the policy cannot be justified in its present blanket form. The infringement of prisoner's rights to maintain confidentiality of their privileged legal correspondence is greater than legitimate public objectives of searching illicit material. Common law gave him privilege to keep his communication with his legal advisor confidential. To search the papers regarding this is breach of his right. The rights of the prisoner can be curtailed clear and express words, and then only to extent reasonable necessary to meet the ends which justify the curtailment and it should not be disproportionate to rights of person."[233]

5.5.2 Right against Breach of Confidence

In **Ashberton** [234], the case was for opposing bankruptcy proceedings against Pape. In this case, Pape wanted to submit some letters written by solicitor of Mr. Ashberton in evidence. Pape sought these letters by sending subpoena to Mr. Brooks, a clerk of the solicitor. Ashberton wanted to seek injunction against such submission on the ground that they were holding privileged communication between his solicitor and him and matter written in it cannot be divulged in. Court had granted injunction as this correspondence is personal nature and it was termed as privileged communication.

In **Saltman Engineering Co (1948).**[235], the plaintiff company conceived idea for leather punches. It asked another company to draw a design for such punches. This second company gave this job to the defendant company and asked it to manufacture the dies according to the plans drawn by second company. The defendant company then used the information of these punches to produce them and sell them themselves. The plaintiff sued defendants for

[233] R (Daly) v. Secretary of State for Home Department (2001) 2 AC 532.at https://publications.parliament.uk/ (Last visited on December 10, 2019)
[234] Ashberton v. Pape 2 Ch.. 469 (C A.) (1913)
[235] Saltman Engineering Co. v. Campbell Engineering co. 3 All E.R 413(1948) 65, RPC 203at https://swarb.co.uk/

breach of confidential information obtained from plaintiff and breach of plaintiff's rights. The court held that the defendants knew that the information was kept in to their possession for the limited purpose of making tools, the tools which were required to make leather punches. Therefore the information was confidential one as it is not public property or public knowledge and defendants used it without consent of the plaintiff. The court allowed a breach of confidence against a larger universe of people who shared confidential relationship.

The defence of breach of confidence is used in **Argyll (1967)**[236] Duke of Argyll married in 1951 to Margaret who became third wife of Duke Argyll. She was known for her extraordinary beauty. Duke Argyll became suspicious that she was unfaithful to him. He employed locksmith to break open the cupboard at their Mayfair apartment and found Polaroid photographs showing the Duchess nude with two other persons. On this basis, in 1963 he wanted to seek divorce. Case was filed and while arguing for the divorce he presented the photos which were taken showing Margaret engaged with other men in very indecent situations. The case was highly contested. He attempted to disclose evidence of his wife's photos and letters to press. Duchess filed for injunction against him and the editor of the paper which was going to publish it. Court granted the injunction. The concept of confidentiality was applied to protect the privacy of communication between the husband and wife. The court observed that "there could be hardly anything more intimate or confidential than mutual trust and confidences which are shared between husband and wife. The confidential nature of the relationship is of its very essence and so obviously and necessarily implicit in a marital relationship."[237]

But when can we say that the information was confidential and disclosing it is an offence? In **Coco (1969)**[238]Court gave test for the breach of confidence. In this case, the plaintiff had designed a moped engine. They discussed this design with defendant with a motive to get co-operation of them in manufacturing it jointly. In the discussion, plaintiff had disclosed the full details of the design of the engine and both of them dispersed. Afterwards, defendants decided to

[236] Argyll v. Argyll Ch. 302, U.K. (1967) at https://swarb.co.uk (Last visited on December 10, 2019)
[237] Argyll v. Argyll Ch. 302, U. K. (1967), at https://swarb.co.uk (Last visited on December 10, 2019)
[238] Coco v. Clark R.P.C 41 U.K (1969), at https://swarb.co.uk (Last visited on December 10, 2019)

manufacture their own engine. Plaintiff brought an action for injunction alleging that defendants have deliberately broke off with them and manufactured the engine which closely resembled the design, using the confidential information shared with them with a motive to manufacture it jointly. Here the court had to decide whether the information shared was a confidential one.

Megarry J. had provided three tests for deciding whether the relationship between the parties have that of confidence. 1. Information must have the necessary quality of confidence about it, 2. It must have been imparted in circumstances imparting an obligation of confidence and 3. There must be an unauthorised use of that information to the detriment of the party communicating it.[239] Meggary J. held that "Whether it is described as originality or novelty or ingenuity or otherwise, I think that there must be some product of the human brain which suffers to confer a confidential nature upon the information." [240]Court held that the information was not satisfying the tests therefore the plaintiff's action failed.

In England, Law of privacy revolved around privacy violations as consequences of breach of confidence. Historically, the law of confidence arose only in special well known relationship of trust or in commercial trade secret context. Though England is signatory to the European Convention, the right to privacy is not enacted under the English law. Person's right to protect his reputation is recognised in action for defamation but not for right to privacy.

5.5.3 Photographs and Right to Privacy

In **Kaye (1991)[241]** the actor Kaye was hospitalised after car accident. He had received severe injuries to his head and brain. With the fear of impediments in his recovery and to lessen the infections, notice was put outside his room regarding restrictions on visitors' entry to meet him. Two journalist-one of them was photographer- invaded his room in hospital and tried to interview him and intended to take photograph. Plaintiff gave consent for interview. The defendants wanted to publish it. This action was challenged on the ground that

[239] Coco v. Clark, R.P.C. 41 U. K. (1969) at https://swarb.co.uk (Last visited on December 11, 2019)
[240] Coco v. Clark, R.P.C. 41 U.K. (1969), at https://swarb.co.uk (Last visited on December 11, 2019)
[241] Kaye v. Robertson (1991) FSR 62, (1990) EWCA Civ.21 at www.bailii.org/ew/cases/EWCA/Civ/1990/21.html (Last visited on December 11, 2019)

plaintiff was not in position to give consent to give interview and photograph. The action was brought for injunction of publishing the photo and interview. Court held that law of trespass would not be applicable as plaintiff was not the owner of the place and his body was not touched. It was held that there is no right to privacy and only remedy available is under malicious falsehood as journalists falsely represented that the plaintiff had consented for the interview.[242]

In **Douglas**[243] and series of cases by the claimants, right to privacy was not confirmed in first case. In the first case in 2001, issue of injunction for publication of photos of Michel Douglas and Catherine Zeta-Jones was involved. In the marriage ceremony of Michel Douglas and Catherine Zeta-Jones, they agreed to give permission to OK magazine regarding the photographs of wedding exclusively and entered into contract with OK magazine. The guests were instructed not to carry any device which is able to take photo. The media was not permitted to attend the wedding. But freelance photographer and son of one of the guests took the photographs and sold it to Hello! Magazine. Douglas and Zeta-jones filed for injunction, prohibiting the magazine Hello! publishing the pictures. Douglas and OK magazine claimed breach of confidence, invasion on right to privacy and breach of Data Protection Act, 1998. High court granted the injunction but Court of Appeal discharged it holding that there is no breach of privacy. It was held that there is no privacy at wedding where 250 guests attended it[244]. The Hon'ble judge held that there must be an obligation of confidence between the parties, and which arises only on private occasions. The court held that damages would be the proper remedy for this breach.

In Douglas (2003)[245] Douglas and OK magazine have succeeded in an action of breach of confidence against Hello! Ltd., company producing Hello!, its Spanish

[242] Kaye v. Robertson, 62 FSR (1991)at www.bailii.org/ew/cases/EWCA/Civ/1990/21.html. (Last visited on December 7, 2019)
[243] Douglas v. Hello! (2001) 2 All E.R. 289 at https://www.bailli.org/ew/cases (Last visited on December 7, 2019)
[244] Douglas v. Hello! (2001) 2 All E.R. 289. at https://www.bailli.org/ew/cases (Last visited on December 11, 2019)
[245] Douglas v. Hello! , (2003) EWHC 786 (Ch),at www.bailii.org/ew/cases/EWHC/Ch/2003/786.html (Last visited on December 11, 2019)

controlling company Hola!, SA and Eduardo Sanchez Junco, Director and controlling shareholder in Hola! SA and Editor-in-Chief of Hello! Magazine.

In Douglas (2005)[246], the claimants-OK magazine and Douglas claimed damages on breach of confidence. The issue before the court was whether OK and Douglas had right to commercial confidence over the wedding photos which were published. After hearing the sides and evidence on record, Court came to conclusion that law of confidence covers the right to privacy and Douglas and OK magazine were entitled to a commercial confidence over wedding photos as the photos were not publicly available, so they were confidential. The court recognised that publication of photos is more intrusive. Moreover, as the contract was entered into with OK magazine allowing them to publish the photos exclusively and OK magazine had suffered monetary loss because of intentional interference of Hello! Magazine. The photographs had commercial value therefore they required confidentiality. Even though OK had published the photos before Hello! magazine, this does not mean photos were in public domain and so did not require confidentiality. Action for breach of confidence succeeded.

They appealed in House of Lords, where Lord Hoffman held that 'right to privacy is not available in England as it is too uncertain'. It was held that claim of protection under Art. 8 of Convention is also not available as it is only a guideline for the common law. He held that "European Court is concerned only with whether English law provides adequate remedy in a specific case in which it considers there has been an invasion of privacy contrary to Art. 8(1), and not justifiable under art. 8(2), and English common law has sufficient privacy protections like breach of confidence. It was also held that after Human Rights Act, 1998, came in to force the argument is weakened that general tort of privacy is needed to fill the gaps."[247] The appeal was dismissed.

[246] Douglas v. Hello! , (2005) EWCA Civ. 95 at www.bailii.org/ew/cases/EWCA/Civ/2005/595.html (Last visited on December 11, 2019)

[247] Wainwright v. Home Office, (2003) UKHL 53, (2003)3 All E R 969, para. 32, 33, 34, html version of judgement at https://publication.parliament.uk/pa (Last visited on December 5, 2019)

In **A v. B Plc, (2002)[248],** i.e. Flitcroft v. MGN Ltd., Premiership Footballer engaged in extramarital relationship with two other women. He sought an injunction to prevent the newspaper from disclosing information concerning sexual relationship that he had with these women and to restrain any disclosure by these women to anyone. The issue was whether to grant injunction as it may interfere the freedom of press and balancing the personal interest and rights under Art. 8 of ECHR. Court granted the interim injunction. The judge held that law of confidentiality shall protect the sexual relations outside the marriage as it protects within the marriage.

B filed an appeal to vacate the injunction on the ground that it affects the freedom of expression as he is restrained from printing the news in newspaper and also a judge had wrongly interpreted s. 12 (4) of Human Rights Act 1998. The appeal was allowed.

While giving the decision, Lord Woolf remarked, "A public figure is entitled to a private life. However he should recognise that because of his public position he must expect and accept that his actions will be mere closely scrutinised by media."[249]

In **Ellis (2003)[250]** , a scheme initiated by Sergeant Quinnel incharge of Burglary and Motor crime section, Essex police of publishing the names and photos of the offenders, motive of which is for reducing core crimes like burglary and car crime. The scheme involved publishing posters in train stations and other travel locations such as garages etc. Protocol for publishing the photos of offenders, scheme provided that offenders serving minimum twelve months in prison should be selected for inclusion in the scheme. The offender and his legal representative were to be given notice on the day of sentencing and given 7 days to register objections against inclusion of their names. The service officer shall approve the scheme. The approval shall be given after consulting the probation services and social services and doing risk assessment for implementation of the

[248] A v. B Plc, QB 195(2002), EWCA Civ. 337. At www.bailii.org/ew/cases/EWCA/Civ/2002/337.html (Last visited on December 7, 2019)
[249] A v. B Plc, QB 195(2003), EWCA Civ. 337 at www.bailii.org/ew/cases/EWCA/Civ/2002/337.html (Last visited on December 5, 2019)
[250] Ellis v. Chief Constable, Essex Police, (2003) EWHC 1321 at www.bailii.org/ew/cases/EWHC/Admin/2003/1321.html (Last visited on December 5, 2019)

scheme. The local authority, probation service and National Association for Care and Resettlement of Offenders (NACRO) had expressed reservations.

E, an offender, was selected to be used for the scheme. Probation service concluded that use of E's name would increase his risk of harm to public, his parents, his ex-partner and his daughter. The police disagreed. Police subsequently decided to withdraw E from the scheme.

The scheme was challenged as being unlawful. The Court had to decide whether the scheme was lawful in nature. All parties agreed that scheme was an interference with right in respect of privacy and family life contrary to Art. 8 of European Convention. Essex police argued the interference is justified under Art. 8 (2) as being necessary in interest of prevention or detection or crime or protection of right and freedom of others.

The court noted that the scheme is unfair to some degree as it discriminate between the offenders selected for the scheme and which are not selected. "But legality or illegality depends upon the facts and circumstances of each case and how the scheme is implemented. The court said that more information is needed to assess the risk involved in scheme. The information would be needed before it could be assessed whether the possible benefits of the scheme was proportionate to the intrusion into offender's right under Art. 8."[251]

In **Campbell (2004)**[252], a famous model Naomi Campbell was photographed coming out of Narcotics Anonymous meeting. The daily 'Mirror' (Mirror Group Newspapers Ltd.) published these photos with faces of other attendees pixelate to protect their identities. The headlines along with the photo of Ms. Naomi was published. The article contained the information about Ms. Campbell's treatment for drug addiction along with the Narcotics Anonymous meetings she attended in very general terms. Ms. Campbell claimed damages for breach of confidentiality and compensation under s. 13 of Data Protection Act, 1998 for publication of further details. She claimed that her photo of coming out of the

[251] Ellis v. Chief Constable, Essex Police, (2003) EWHC 1321.at www.bailii.org/ew/cases/EWHC/Admin/2003/1321.html

[252] Campbell v. MGN Ltd., UKHL 22. (2004) at www.bailii.org/uk/cases/UKHL/2004/22.html (Last visited on December 5, 2019)

Narcotics Anonymous will deter other people accessing the place with fear that they also will be photographed.

This additional information is a breach of confidence under s. 6 of Human Right Act, 1998. High court upheld the claim and held MGN liable and awarded damages. Court of Appeal reversed the decision. Ms. Campbell challenged this. House of Lords held MGN liable for the breach by majority. Baroness Hale held that picture added impact to the information[253]. House of Lords considered the balancing test of the rights of concerned parties. She had considered and weighed that whether there was reasonable expectation of privacy by claimant as information of Ms. Campbell's addiction and treatment is important aspect of the physical and mental health and this information is received from breach of confidence.[254] Lord Hope held, "She would have seen their publication, in conjunction with the article which revealed what she had been doing when she was photographed and other details about her engagement in the therapy, as a gross interference with her right to respect her private life. This additional element in the publication is more than enough to outweigh the right to freedom of expression which is the defendant asserting in this case." [255]This privacy right under art. 8 is interfered by publishing the news under freedom of expression under Art. 10 of the convention. It was held that Campbell's right to privacy outweighed the MGN's right to freedom of expression[256].

In **Mosley (2008)**[257] president of Federation of International de Automobile, the governing body of motor sport worldwide, was filmed engaging in sadomasochistic activities with five hookers in a private flat. An edited version of the footage was made available on NGN's website with a news of world. Article was published with the title 'F1 Boss has sick Nazi orgy with 5 hookers'. After the objection was taken the Newsgroup has removed the clip from website

[253] Campbell v. MGN Ltd., UKHL 22. (2004), para. 155, at www.bailii.org/uk/cases/UKHL/2004/22.html (Last visited on December 5, 2019)
[254] Campbell v. MGN Ltd., UKHL 22. (2004), para. 147, 148, at www.bailii.org/uk/cases/UKHL/2004/22.html (Last visited on December 4, 2019)
[255] Campbell v. MGN Ltd., UKHL 22. (2004), para. 124., at www.bailii.org/uk/cases/UKHL/2004/22.html (Last visited on December 5, 2019)
[256] Campbell v. MGN Ltd., UKHL 22. (2004), para. 169, 170, at www.bailii.org/uk/cases/UKHL/2004/22.html (Last visited on December 5, 2019)
[257] Mosley v. News Group Newspapers Ltd. (2008)EWHC 1777 QB at www.bailii.org/ew/cases/EWHC/QB/2008/1777.html

but before removal millions of people had already watched it. Mosley has accepted that events shown occurred but claimed that their disclosure infringed his right to privacy. He also denied Nazi element.

The issues involved was whether the disclosure of sexual activities based on Nazi theme was in public interest and fit for protection of publishing and whether such disclosure is in breach of privacy of claimant. The Court came to the conclusion that there was no evidence that sexual role-play was intended to be enactment of Nazi behaviour or adoption of any of its attitudes. Those sexual activities were unconventional therefore there was no public interest in showing them and no other justification is available.

For publication in 'public interest', the court held that, "I have come to the conclusion that if it really were the case, as the newspaper alleged, the claimant had for entertainment and sexual gratification been mocking the "humiliating way the Jews were treated" or "parodying Holocaust horrors", there could be a public interest in that being revealed at least to those in the FIA to whom he is accountable. ..On the other hand, since I have concluded that there was no such mocking behaviour and not even, on the material I have viewed any evidence of imitation, adopting or approving Nazi behaviour, I am unable to identify any legitimate public interest to justify either the intrusion of secret filing or the subsequent publication."[258]

It was held that "Claimant had a reasonable expectation of privacy in relation to sexual activities carried on between consenting adults on private property. There is no evidence that the gathering was intended to be an enactment of Nazi behaviour or adoption of any of its attitudes."[259] There is breach of privacy of the Footballer.

In **AAA v. Associated Newspapers Ltd.(2012)**[260] , the claimant is a child born in 2009 of unmarried art professional consultant. The news was published in Daily Mail about the claimant's paternity with the photograph on 16th July 2010.

[258] Mosley v. News Group Newspapers Ltd. (2008)EWHC 1777 QB. Para.122, 123, at www.bailii.org/ew/cases/EWHC/QB/2008/1777.html (Last visited on December 4, 2019)
[259] Mosley v. News Group Newspapers Ltd. (2008)EWHC 1777 QB. Para. 232. At www.bailii.org/ew/cases/EWHC/QB/2008/1777.html (Last visited on December 4, 2019)
[260] AAA v. Associated Newspapers Ltd. (2012) EWHC, 2103 (QB), at www.bailii.org/ew/cases/EWHC/QB/2012/2013.html (Last visited on December 4, 2019)

Before this, the personal information was not in public domain. Her alleged father is prominent elected politician. To get more detailed news, media hounded her mother. Claimant challenged this contending that publication of private information is a breach of her rights under Art. 8. It was contended that she had reasonable expectation of privacy in respect of the information about her paternity. Defendant contended there is public interest in the news and it has freedom of expression and right under art. 10 of the convention.

After going through the evidence on record, it was observed by the court that mother of the claimant had told the information about the paternity of her child and revealed the name of the father at the garden party in June 2010 to her friends i.e. before publication. Court held that this compromised reasonable expectation of privacy of the claimant. For public interest, court held that "It is not in dispute that the legitimate public interest in the father's character is an important factor to be weight in the balance against the claimant's expectation of privacy. The core information in this story, namely that the father had an adulterous affair with the mother, deceiving both his wife and mother's partner and that of claimant born bout 9 months later was likely to be father's child, was a public interest matter which the electorate was entitled to know when considering his fitness for high public office." [261]So this fulfils the criteria of 'publication in public interest' under art. 10 of the convention.

But as the private information was disclosed by the mother, reasonable expectation of privacy of the claimant is lessened in effect and so the publishing the information about the alleged politician father regarding his character, his recklessness etc. are justified.[262] The court decided against the claimant.

The claimant filed an appeal against the order. The court had affirmed the judgement given by the high court.[263]

[261] AAA v. Associated Newspapers Ltd. (2012) EWHC, 2103 (QB) at www.bailii.org/ew/cases/EWHC/QB/2012/2013.html (Last visited on December 4, 2019)
[262] AAA v. Associated Newspapers Ltd. (2012) EWHC, 2103 (QB) at www.bailii.org/ew/cases/EWHC/QB/2012/2013.html (Last visited on December 4, 2019)
[263] AAA v. Associated Newspapers Ltd. (2013) EWCA, Civ. 554 at www.bailii.org/ew/cases/EWCA/Civ/2013/554.html (Last visited on December 4, 2019)

Weller v. Associated Newspapers Ltd.(2014)[264] where Associated Newspapers was defendant, which misused the photographs taken without the consent. Paul Weller, a well-known musician and his children went to Santa Monica, Los Angelis, California. An unknown photographer took the photos of all shopping on the street and relaxing at the café. The article was published by Associated Newspapers Ltd. on its Mail Online website. The article contained the description of content and photos. It also described the activities carried out by all of them. In the article and caption below the photo, one child aged 17, was described wrongly as Hanna, wife of Weller. Due to the mistake in the description, the article was removed from the website. But the website has substantial viewership. Action was damages was filed by Claimants for misuse of private information and breach of Data Protection Act, 1998. They contended that pictures of their faces should have been 'pixelated'.

Court considered various relevant principles of law for deciding the issues. The first issue was whether there is a reasonable expectation of privacy. For answering this court referred the cases especially of Murray v. Express Newspapers plc. (2008) EWCA Civ. 446 (2009) Ch. 481 which provides that reasonable expectation of privacy "need to be known or ought to be known" and held that there was a reasonable expectation of privacy. The publisher new that the photos had been taken without consent and faces in the photos shows emotions that they are on family trip, they are with their father shopping and relaxing at caffe. They were reasonably expecting privacy.[265] As the photos were taken in Santa Monica, Los Angelis, California, the court referred the law pertaining to clicking photographs and publishing them in California. But as the publication by Mail Online occurred within the jurisdiction of England and Wales, it considered the law of England.

For second issue whether there was a public interest in publishing the photos. The court referred Van Hannover v. Germany (No.2) (2012) 55 EHRR 15 case and held that applying those standards the balance is in favour of the claimant. The publication of children's faces showing the emotions on the family

[264] Weller V. Associated Newspapers Ltd. (2014) EWHC 1163 (QB) at www.bailii.org/ew/cases/EWHC/QB/2014/1163.html (Last visited on December 4, 2019)
[265] Weller V. Associated Newspapers Ltd. (2014) EWHC 1163, Para. 170 at www.bailii.org/ew/cases/EWHC/QB/2014/1163.html (Last visited on December 4, 2019)

afternoon out with their father. The publication of the photos did not contribute for the public knowledge and interest of the children outweigh the interests of the publication so their publication is not in public interest.[266] So defendant is liable under Data Protection Act, 1998 as privacy claim of the claimant is established.[267]

Substantial amount of damages 10,000 Pounds were awarded (5,000 pounds for Dylan, 2,500 pounds for John Paul and 2,500 pounds for Bowie-both twins.)[268]

In **Cliff Richard (2018)**[269] South Yorkshire police officers were investigating an allegation made by a man, who claimed that he was sexually assaulted by Sir Cliff, 77 years old singer, at an event in 1985, when he was a child. BBC reporter came to know about this and contacted the police. Police affirmed the fact and agreed to give information in advance about raiding the property. Police raided his home in August, 2014. BBC arranged journalists to attend and a helicopter was hired to film the search. BBC used helicopter pictures while reporting the news and the news were broadcasted at lunch time and Sir Cliff was identified. Police made a statement but did not name Cliff. Millions of viewers observed the news.

The coverage had a serious emotional and physical effects on Sir Cliff. He was investigated till 2016 but no charges were brought.

Sir Cliff sued BBC and South Yorkshire Police for breach of his right to privacy under Human Rights Act and Data Protection Act, 1998. To decide the right of Sir Cliff, court verified various cases regarding reasonable expectation of Privacy of him.[270]. BBC argued that the Human Rights Act protects freedom of expression[271]. Court held that every suspect has right of reasonable expectation of privacy in relation to police investigation as suspect does not want others to

[266] Weller V. Associated Newspapers Ltd. (2014) EWHC 1163, Para. 182 at www.bailii.org/ew/cases/EWHC/QB/2014/1163.html (Last visited on December 4, 2019)
[267] Weller v. Associated Newspapers Ltd. (2014) EWHC 1163, para. 184 , at www.bailii.org/ew/cases/EWHC/QB/2014/1163.html (Last visited on December 4, 2019)
[268] Weller V. Associated Newspapers Ltd. (2014) EWHC 1163 Para. 197, at www.bailii.org/ew/cases/EWHC/QB/2014/1163.html (Last visited on December 4, 2019)
[269] Cliff Richard v. BBC (2018). EWHC 1837 (Ch)
[270] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.) Para 227, approved judgement at https://www.judiciar.uk (Last visited on December 1, 2019)
[271] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.)Para 228 approved judgement at https://www.judiciar.uk (Last visited on December 1, 2019)

know because of stigma attached.[272] Though Sir Cliff is public figure, he has right of reasonable expectation of privacy with regard to BBC[273]. Even though the information is private, until it is disclosed, it does not change its quality of being private[274]. Journalist knew that this information is confidential and it was not obtained in straight forward manner. BBC did not give Sir Cliff or his representative a fair opportunity to clarify before publication.[275]

Moreover it was held that "the content engaged in broadcasting attracts the Art. 8 of the convention as it is sensationalised using helicopter footage. This sensation resulted in serious consequences".[276] This sensationalist style of reporting weighed against Art. 10 because it materially increase the impact on invasion of privacy[277].

Judge held that recovering damages to reputation is possible in privacy action and the factors taken in to consideration are a. damages for distress, damage to health, invasion of privacy as well as to dignity, status, and reputation b. adverse effects on lifestyle, c. significant nature and content of private information revealed (more private, more significant), d. scope of publication, e. presentation of publication[278]. It was held that "effects on Sir Cliff were strong, content was extremely serious and publication was worldwide. The coverage was sensational to the extent of making a hype"[279]. Therefore the Court held in favour of Sir Cliff and damages of 190,000 pounds were awarded to him[280].

5.5.4 Right to Protection of Data

[272] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.)Para 248 approved judgement at https://www.judiciar.uk (Last visited on December 1, 2019)
[273] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.)Para 256-257, 261 approved judgement at https://www.judiciar.uk (Last visited on December 1, 2019)
[274] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.)Para 258 approved judgement at https://www.judiciar.uk(Last visited on December 1, 2019)
[275]Cliff Richard v. BBC (2018). EWHC 1837 (Ch.) Para. 293,294 approved judgement at https://www.judiciar.uk (Last visited on December 1, 2019)
[276] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.).Para. 300 approved judgement at https://www.judiciar.uk
[277] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.).Para 301 approved judgement at https://www.judiciar.uk
[278] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.) Para. 350 approved judgement at https://www.judiciar.uk (Last visited on October 11, 2019)
[279] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.).Para. 351- 357 at https://www.judiciar.uk(Last visited on October 11, 2019) (Last visited on October 11, 2019)
[280]Cliff Richard v. BBC (2018). EWHC 1837 (Ch.) Para. 358. At https://www.judiciar.uk (Last visited on October 11, 2019)

The power of collection of fingerprints, DNA samples and other material of the accused is granted to police officers of every country under legal provisions. In England, since 2004, the collection of fingerprints, DNA samples are used to taken by police officers and even if the case is dismissed or accused is acquitted, such samples of evidence are kept permanently. There is a blanket power of retention. It is retained irrespective of nature or gravity of offence or irrespective of age of suspect or criminal. It is also not time limited.

This power was challenged on the ground of 'breach of right to privacy' in **S and Marper's**[281] case. In this case S was arrested in 2001 at the age of eleven. He was charged with attempted robbery. His finger prints and DNA samples were taken. Subsequently he was acquitted. The second applicant Mr. Marper was arrested in 2001 and charged with harassment of his partner. His finger prints and DNA samples were also taken. At pre-trial review, he and his partner reconciled, charges were not pursued and in June 2001 the case was formally discontinued. Both the applicants asked for their finger prints and DNA samples to be destroyed under s. 64 of Police and Criminal Evidence Act, 1984(after it is amended in 2001). This Act provides that Chief Constable has power to retain finger prints and DNA samples irrespective of the outcome of the proceedings, except for some specific reasons the Chief Constable is asked to destroy them in particular. Police refused to do so.

Both of them applied for judicial review of decision of the police not to destroy by challenging it. They contended that retention of fingerprint and DNA samples is breach of their right to privacy under art. 8 of the Convention. The court examined the contention on the issues a). whether retention under s. 64 is interference and it offends the right to privacy under art. 8(1) and whether it is saved by art. 8(2), and b. whether it offends art. 14 of the convention. Art. 8 (1) provides that 'Everyone has the right to respect for his private and family life, home and correspondence', and art. 8 (2) public authority can only restrict it in accordance with the law and is necessary in democratic society.

Court held that the law under s. 64 is very clear that chief constable has discretionary power to decide whether to destroy or not which he had exercised

[281] S and Marper v. UK (2002) EWHC 478, Admini, (2003) EWCA Civ. 1275, (2004) House of Lords.

it in accordance with law and there is no lack of clarity[282]. For 'necessity' in democratic society under art. 8(2), court held that restriction is justified and termed as necessary for pressing social need, which is provided under the object of the provision as it is for prevention and detection of crime and pressing necessity of combatting terrorism[283]. Restriction shall be proportionate also. Court decided the issue of proportionality of the restriction considering the various decided cases. "The restriction is proportionate if legislative objective is sufficiently impart to justify limiting the fundamental rights, measures designed to meet the legislative objective are rationally connected to, and the means used to impair the right or freedom are no more than is necessary to accomplish the objective" as held by Gubbay CJ in Nyambirai v. National Social Security Authority, (1996) 1 LRC 64.p.75"[284] So this legislation is proportionate.

Regarding 'interference' in rights under art. 8(1), Court held that "unless something form the crime scene, which matches positively with samples at level acceptable to an expert, the fact that his finger prints and samples are in data base will simply not impact on person from whom they were taken. Thus availability of sample will serve to assist in the elimination of most and will only focus on someone who is, in fact, implicated."[285] So "the legislation is proportionate."[286] In 2002, Administrative division of High Court rejected the application.

In September, 2002, Court of Appeal upheld the decision of Administrative division of High Court in 2003 Judge referred the observations made in cases of R. v. B and R. v. Weir,(1992/4829/w.2) and also referred the arguments in House of Commons relating to art. 8(2). The Court held that "amendment is lawful as collection of fingerprints and DNA samples are according to principles

[282] S and Marper v. UK (2002) EWHC 478, (Admin), Para. 27, at www.bailii.org/ew/cases/EWHC/Admin/2002/478.html (Last visited on October 11, 2019)
[283] S and Marper v. UK (2002) EWHC 478, (Admin),Para.34, at www.bailii.org/ew/cases/EWHC/Admin/2002/478.html (Last visited on October 11, 2019)
[284] S and Marper v. UK (2002) EWHC 478, (Admin), para.29, at www.bailii.org/ew/cases/EWHC/Admin/2002/478.html (Last visited on October 11, 2019)
[285] S and Marper v. UK (2002) EWHC 478, (Admin), para. 33, at www.bailii.org/ew/cases/EWHC/Admin/2002/478.html (Last visited on October 11, 2019)
[286] S and Marper v. UK (2002) EWHC 478, (Admin),. Para.34,at www.bailii.org/ew/cases/EWHC/Admin/2002/478.html (Last visited on October 11, 2019)

art. 8 (1). Also the fingerprints and samples are used only for the purpose of prevention and detection of crime, the investigation of offence, and conduct of prosecution. Language is very similar to art. 8 (2)."[287]So law is compatible and does not interfere with the rights of the person under art. 8 (1). In 2004, House of Lord upheld the issued decided by the courts[288] and dismissed the appeal.

The decision was challenged before European Court of Human Rights. The court verified the facts and provisions in English law and came to the conclusion that retention of such samples without any justified cause is breach of privacy as provided under Art. 8 of the Convention as DNA samples, fingerprints etc. constitute 'personal data' under it.

Information and data relating to an individual has become valuable in cyber society. Therefore violation of privacy of personal data or information and its protection has become more difficult in current situation. Publication of personal information was held violation of right to privacy under the provisions of Human Rights Act and Data Protection Act in many cases in recent years. Some of the leading cases are discussed here.

For data privacy the leading case is **Halliday(2013)** [289] where claimant was awarded 750 Pounds for wrongful processing of his data. Mr. Halliday purchased T.V. and entered into a credit agreement with Creation Consumer Finance Ltd. There were complex development in events and Creation Consumer Finance Ltd. (CCF) had shown wrongly that Halliday owed money to it. This wrong information was shared with credit reference agency. He brought proceedings against Creation Consumer Finance Ltd. (CCF) for breach of Data Protection Act, 1998. He claimed the damages for harm to his reputation and credit rating.

At the hearing for assessment of damages, judge awarded nominal general damages and not actual quantified loss. He held that there is no power under s.

[287] S and Marper v. UK (2002) EWCA Civ. 1275,para.39, 69, at www.bailii.org/ew/cases/EWCA/Civ/2002/1275.html (Last visited on October 9, 2019)
[288] R.v. Chief Constable of South Yorkshire police (Res.) ex parte LS (by his mother and litigation friend JB) (FC) and R. v. Chief Constable of South Yorkshire police (Res.) ex parte Marper (FC) Consolidated appeal.(2004) UKHL 39, https://publications.parliament.uk/ (Last visited on October 9, 2019)
[289] Halliday v. Creation Consumer Finance Ltd. (2013)EWCA Civ. 333(2013) at www.bailii.org/ew/cases/EWCA/Civ/2013/333.html (Last visited on October 9, 2019)

13 of Data Protection Act, 1998 to award compensation for distress. The damages can be awarded if damages are suffered by reason of contravention for requirement for processing the data and is suffered by the complainant himself. Halliday filed an appeal.

Court of Appeal held that nominal damages can be awarded where claimant cannot prove actual loss and such remedy is appropriate for the purposes of European Union Law. The court reviewed whether damages for distress can be claimed. It was held that there is no proof that CFF had acted with malicious or fraudulent intention. But non-compliance with the European law will cause frustration to complainant and therefore compensation for such frustration may amount to as little as 750 pounds.

Arden J said, "it was a general principle that where an important instrument such as data protection had been complied with, there ought to be an award. Even though there was no contemporary evidence of manifestation of injury to feelings and distress output from what one could normally expect from the frustration of these prolonged and protected events"[290].

This final decision created two rules. One in absence of direct evidence of specific financial loss, nominal damages may be awarded for breaches of Data Protection Act, 1998. And secondly, additional remedy for frustration or distress may be awarded.

In **Gulati (2015)**[291], the voicemail messages of the applicants-celebrities- were accessed by intercepting the mails by MGN, proprietor of three publications, Daily Mirror, Sunday Mirror and The People. The phone numbers were obtained from interception, from mobile telephone companies and from private investigators using hacking of the phones of various famous people including actors, sportsmen and persons associated with them. Use of voicemail was such that their personal, family and medical information was disclosed to the outsiders who were hearing while interception. Using the information from this interception, articles were written and published in the newspaper. This misuse

[290] Halliday v. Creation Consumer Finance Ltd. (2013)EWCA Civ. 333(2013) at www.bailii.org/ew/cases/EWCA/Civ/2013/333.html (Last visited on October 9, 2019)
[291] Gulati v. MGN Ltd. (2015) EWHC 1482 (Ch) at www.bailii.org/ew/cases/EWHC/Ch/2015/1482.html (Last visited on October 9, 2019)

of private information was challenged and trial was for fixing the quantum of damages.

The defendant admitted that most of the articles were the product of this hacking. The trial is not only for hacking activities which were resulted in articles but the claims were also based on hacking which did not result in articles.[292]

Mann J held that where defendant had helped itself to large amounts of personal and private information and treated it as its own to deal with as it thought fit, there was a serious infringement. The invasion was on large scale, and daily for getting the material for writing the articles. For awarding compensation, damages awarded in referred cases were considered and he was of the opinion that damages were less as gravity of invasion was less. Generally damages are awarded for injury to feelings, but aggravating factors caused greater hurt and thus increased damages are awarded.

He held that for aggravated damages things contributed mainly, i) the manner in which the wrong was committed i.e. systematic, long standing and widespread, ii) covert nature, iii) subsequent conduct of the defendant[293]. The court held that "awards of damages in this case are substantial than any hitherto reported privacy cases. The fact that they are greater than any other publicly award result from the fact that the invasions of privacy involved were so serious and prolonged. That hacking existed in all case whether or not an article resulted. The length, degree and frequency of all this conduct explains why the sums I have awarded are so much greater than historical award. People whose private voicemail messages were hacked so often and for so long and had very significant parts or their lives exposed and then reported on, are entitled to significant compensation."[294] It was argued by the defendant that the damages are vindicatory, but court opined the extent of publication of private information is relevant to the level of damages. Assessment of damages were done in eight

[292] Gulati v. MGN Ltd. (2015) EWHC 1482 (Ch), para. 3 at www.bailii.org/ew/cases/EWHC/ch/2015/1482.html (Last visited on October 9, 2019)
[293] Gulati v. MGN Ltd. (2015) EWHC 1482 (Ch), Para. 207, www.bailii.org/ew/cases/EWHC/ch/2015/1482.html (Last visited on October 9, 2019)
[294] Gulati v. MGN Ltd. (2015) EWHC 1482 (Ch), para. 702 www.bailii.org/ew/cases/EWHC/ch/2015/1482.html (Last visited on October 9, 2019)

cases and awards between 72,500 Pounds and 260,250 Pounds were given. So in this case the aggravated damages were awarded to the claimants.

It was held in **Vidal-Hall (2015)**[295] that compensation could be awarded to individual under English law if they suffered non-pecuniary loss such as distress arising from a breach of data protection legislation. In this case, it was alleged by three British persons that their personal information about their internet usage was collected by Google through Apple Safari browser and this information was supplied to advertisers as per its commercial contract. The claimants sought damages for anxiety and distress but did not ask for any pecuniary loss.[296]

The Court of Appeal had number issues, but mainly it had to decide that whether the meaning 'damage' provided under s. 13 of UK Data Protection Act, 1998, permits claims for compensation without showing proof of pecuniary loss. While interpreting s. 13, Court of Appeal referred Art. 23 of the EU Directive 95/46[297], which is the basis of UK Data Protection Act, 1998, and which provides for the person who has suffered the damage due to breach of data protection provisions to receive compensation and held that it includes non-pecuniary damages[298]. The court held that tort of misuse of personal information is tort within the meaning of the ground and claimants' claim fall within that ground.[299]

Google had filed an appeal on this decision[300]. The appellate court held that misuse of private information is tort.[301] For deciding the damages, the court verified the provisions of art. 23 of the Directive 95/46 and s. 13 of Data Protection Act, 1998 and came to the conclusion that both are not compatible. It was held that Directive aims at safeguarding privacy rights in context of data management, which is repeatedly emphasized in recitals.[302] The court held that

[295] Vidal-Hall and Ors. v. Google Inc. (2015) EWCA Civ 311, (2016) QB 1003.
[296] Vidal-Hall and Ors. v. Google Inc. (2014) EWHC 13 QB.
[297] Vidal-Hall and Ors.v. Google Inc. (2014) EWHC 13 QB. Para. 92, www.5rb.com/wp-content/uploads/2014/vidal-Hall-v.-Google.pdf (Last visited on October 9, 2019)
[298] Vidal-Hall and Ors.v. Google Inc. (2014) EWHC 13 QB. Para. 103, at www.5rb.com/wp- content/uploads/2014/vidal-Hall-v.-Google.pdf (Last visited on October 9, 2019)
[299] Vidal-Hall and Ors. v. Google Inc. (2014) EWHC 13 QB. Para. 143, at www.5rb.com/wp-content/uploads/2014/vidal-Hall-v.-Google.pdf (Last visited on October 9, 2019)
[300] Google Inc. v. Vidal-Hall and Ors. (2015) EWCA Civ. 311
[301] Google Inc. v. Vidal-Hall and Ors. (2015) EWCA Civ. 311Para. 51, approved judgement at www.judiciary.uk (Last visited on November 29, 2019)
[302] Google Inc. v. Vidal-Hall and Ors.(2015) EWCA Civ. 311Para. 56-57 approved judgement at

"Art. 23 of Directive must be given its natural and wide meaning so as to include both material and non-material damage."[303] "It does not distinguish between pecuniary and non-pecuniary damages. So no reason to interpret the 'damage' in art. 23 a being restricted to pecuniary damages."[304] So damages can be awarded for distress also. Court dismissed the appeal.

When the damage is suffered by an individual, the compensation can be decided by the court. But where no damage is suffered by an individual, can a compensation be given to him? The issue of use of cookies by the service providers to gather information and then using it for commercial benefit/profit was discussed in Lloyd's case.

In **Lloyd (2018)**[305], question was raised that whether compensation can be awarded where there is no damage or distress is proved. The 'Safari workaround' was the well-known browser for i-phone users. Lloyd, a representative claimant, contended that Google allegedly obtained private information about internet usage through its use of cookies without the knowledge or consent of person via 'Safari web browser'. According to plaintiff, this information enabled Google to provide information to advertisers to help in targeting or tailoring of advertisements to internet users and earn very substantial profit. Claimant sought compensation arising from alleged breaches of data protection principles set out in Data Protection Act, 1998. These breaches were committed by implementation and operation of Safari Workaround. The claimant relied on s. 13 of Data Protection Act, 1998, where data subject can receive compensation if he suffer damages due to contravention by data controller. Here the claimant had to show material (pecuniary) loss or emotional harm such as distress. But he relied on the breach without knowledge or consent of the person, collection and use was contrary to defendant's public

www.judiciary.uk (Last visited on November 29, 2019)

[303] Google Inc. v. Vidal-Hall and Ors. (2015) EWCA Civ. 311Para. 76 approved judgement at www.judiciary.uk (Last visited on November 29, 2019)

[304] Google Inc. v. Vidal-Hall and Ors. (2015) EWCA Civ. 311Para 79 approved judgement at www.judiciary.uk (Last visited on November 29, 2019)

[305] Lloyd v. Google Inc., (2018) EWHC 2599, (2019 QB 1599)

statement and collection and use was greatly to commercial benefit and not on results or consequences of such breach[306].

Court held that, "I do not believe that the authorities show that a person whose information has been acquired or used without consent invariably suffers compensetable harm, either by virtue of the wrong itself, or the interference with autonomy that it involves." [307] Therefore the court dismissed the action and ordered, "Facts alleged in the particular claim do not support the contention that the Representative claimant or any of those who he represents have suffered 'damage' within the meaning of Data Protection Act, 1998."[308]

This was appealed and Court of Appeal allowed the claim[309]. While arriving at the decision the court considered the Directive, its aim, art. 1, 22 and 23 and legal provisions of Data Protection Act, 1998. Court also considered the authorities in this regard and came to the conclusion that claimant can recover damages for loss of control of their personal data under s. 13 of Data Protection Act, 1998, without proving pecuniary loss. [310]

With development in technology, new devices are used to maintain the security of the state. These devices may raise the privacy concern. To what extent use of such devices is valid? This was answered by court in the case of **R. (Bridges) (2019)**[311]. In this case South Wales Police has used Automated Facial Recognition (AFR) Technology for prevention and detection of crime. Use of CCTV camera is basic condition for use of AFR. Digital video recording by CCTV camera is used by AFR technology to isolate pictures of individual faces and to extract information about facial features from those pictures of the persons on the watch list. In AFR technology digital photo of a person's face is taken and processed to extract biometric data (measurements of facial features) that data is then compared with facial bio-data from images contained in data

[306] Lloyd v. Google Inc., (2018) EWHC 2599,Para 23 at www.judiciary.uk/wp-content/upload/2018/10/lloyd (Last visited on November 29, 2019)
[307] Lloyd v. Google Inc., (2018) EWHC 2599,Para74 at www.judiciary.uk/wp-content/upload/2018/10/lloyd(Last visited on November 29, 2019)
[308] Lloyd v. Google Inc., (2018) EWHC 2599,Para.106, at www.judiciary.uk/wp-content/upload/2018/10/lloyd(Last visited on November 29, 2019)
[309] Lloyd v. Google Inc. (2019) EWCA, Civ. 1599
[310] Lloyd v. Google Inc. (2019) EWCA, Civ. 1599
[311] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin)

base.[312] South Wales Police used it to verify the suspects. If no match is found, the data is automatically deleted immediately. Data about the match is retained in AFR up to 24 hours. But it can be preserved up to 31 days.[313]

The Secretary of State for Home Department has provided responsibility for policing and nationwide concern for use of development of legal use of technology. He has provided funding for development of AFR to South Wales Police and issued Biometric Strategy (June 2018). The Information Commissioner has specific statutory powers under Data Protection Act, 2018 and Data Protection Act, 1998.

Use of AFR was challenged by Edward Bridges, a civil liberties campaigner. He submitted that he was present when trial regarding AFR was taken by South Wales Police. In December 2017, at Queen's Street, busy shopping area and in March, 2018 at the time of Defence Exhibition. He had challenged on the grounds that (1) the use of such software is in contravention of Convention Rights under Art.8 of ECHR, (2) against Data protection Acts 1998 and 2018 and therefore illegal.

The court examined the provision of Art. 8 and opined that the application of Art. 8 is not dependant on long term retention of biometric data. It is sufficient that biometric data is captured, stored and processed, even momentarily. The mere storing of biometric data is enough.[314] So mere storing of data relating to private life of an individual amounts to an interference within the meaning of Art. 8 and privacy rights of appellant is affected. But it is also important to verify that whether police has those powers. Court verified the legal provisions and held that "there is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used. What is important is to focus on substance of actions that use AFR Locate entails, not simply that it involves

[312] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin) Para. 23, html version of court at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html (Last visited on November 28, 2019)

[313] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin). Para.37, html version of court at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html (Last visited on November 28, 2019)

[314] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin) Para.59, html version of court at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html (Last visited on November 28, 2019)

first-time deployment by South Wales Police of an emerging technology. The fact that technology is new does not mean that it is outside the scope of existing legislation."[315]

"This legislation had three elements, i) primary legislation-it includes Data Protection Act, 2018 which embeds all key safeguards which apply to processing of data. It includes biometric data processed by AFR. Part 3 of the DPA 2018 applies to processing for law enforcement." [316] ii)"Secondary legislation is Surveillance Camera Code of practice, issued by Home secretary, contains guidance about use of surveillance system.[317] Iii) Third legislation is framework of South Wales Police's own policies as to use of AFR.[318] The Court held that "drawing to these matters together, the cumulative effects of a) provisions of DPA, 2018, b) Surveillance Camera Code and c) South Wales Police's own policy documents, is that the infringement of Art. 8(1) rights which is consequent on South Wales Police's use of AFR, occurs within a legal framework that is sufficient to satisfy the "in accordance with the law" requirement in 8(2)."[319] It was held that " we are satisfied both that the current legal regime is adequate to ensure the appropriate and non-arbitrary use of AFR Locate, and that South Wales Police's use to date of AFR Locate has been consistent with the requirements of Human Rights act and Data Protection legislation."[320] The judicial review was dismissed.

Data protection is an area of importance and complexity. Many issues which are claimed on the basis of Data Protection Act are discussed and decided in **Rudd**

[315] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin) Para.84, html version of court at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html (Last visited on November 28, 2019)
[316] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin) Para.85, html version of court at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html (Last visited on November 28, 2019)
[317] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin) Para.89, html version of court at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html (Last visited on November 28, 2019)
[318] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin) Para.92 at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html (L(Last visited on November 28, 2019) ast visited on November 28, 2019)
[319] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin) Para.96, html version of court at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html (Last visited on November 28, 2019)
[320] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin) Para. 159, html version of court at www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html

(2019)[321] Dr. Rudd was a consultant physician specialised in respiratory medicine and leading expert in asbestos related concern. He has given expert opinion, over 35 years, in the cases in United Kingdom to claimants who sought damages for lung cancer and other diseases caused by exposure to white asbestos.

Mr. Bridle has a career in asbestos industry as manufacturer of the material including asbestos in building materials. He runs websites 'Asbestos Watchdog' for promoting industry's interest. He and his son were controlling a company 'J and S Briddle Ltd.'

White asbestos is banned in European Union from 2005. There were disputes between Dr. Rudd and Mr. Bridle about the effects of white asbestos in various diseases. The claimant alleged that Mr. Bridle, with the help of other unknown persons, was engaged in an attempt to discredit him as a witness and tried to intimidate him. He gave the examples:

1.Mr. Bridle filed a complaint to General Medical Council (GMC) alleging that Dr. Rudd falsified the Expert Reports about risks to health associated with white asbestos. GMC rejected the complaint holding not meeting the standard for the investigation. In review also, this decision was upheld. 2. Mr. Bridle made complaint to member of Parliaments alleging that claimant is involved in conspiracy with various law firms in which he provides false evidence about the risks.

Dr. Rudd sought information about Bridle's activities and which individual or companies are behind complaint. He made an application for Subject Access Request regarding his personal information from Mr. Bridle as data controller as complaint to GMC was sent from e-mail of 'Asbestos Watchdog'. Mr. Bridle contended that J&S Company is data controller and not he personally. He claimed exemption for disclosure on grounds of journalism, regulatory activity and legal profession privilege. Issues out of Data Subject Access Request (SAR) u/s 7 of Data Protection Act, 1998 was filed by Dr. Rudd. Notice was given to provide the information.

[321] Rudd v. Briddle, (2019) EWHC 1986 (QB) at www.bailii.org (Last visited on November 28, 2019)

The Court framed two issues- (a) who is data controller at material time? It was observed that the e-mails sent by Mr. Bridle to GMC had footer referring to company, it was stated that "J&S Bridle Associate Ltd. is the commercial arm of Asbestos Watchdog, UK."[322] Terms and Condition section of Asbestos Watchdog website, since 2011 shows that Asbestos Watchdog is trading name of company.[323] Court came to conclusion that the company's name is used by Mr. Bridle. So the data controller is not company but Mr. Bridle.[324]

(b) Whether data controller has complied with duties under s. 7 for provision of information. The exemptions claimed were (i) journalism-for this, the criteria in Information commissioner's guide for media was to be complied which was not done[325], (ii). regulatory act-it can be for protection of members against dishonesty, malpractice, and other seriously improper conduct of persons having authority to carry on any profession or other activity- this was also not established[326] and (iii) privilege- It is to be shown such information is to be used in any prospective litigation or any other disciplinary action- was not proved.[327] So defendants failed to prove all the grounds taken for the defence. It was held by the court that data controller had not complied with the duties under s. 7 of DPA 1998 and information provided to claimant was inadequate.

5.5.5 Discussion.

It is evident from the cases discussed above, even though Right to Privacy is not provided under British Constitution and under any enacted law, the courts in England protected this right under tortious principles relating to property as observed under Entick (1765)[328] and extended to letters in Gee(1818),[329] and Pope (1741)[330]. But it was held that right to privacy was breached when etchings

[322] Rudd v. Briddle, (2019) EWHC 1986 (QB), Para.149 html version of judgement at www.bailii.org (Last visited on November 24, 2019)
[323] Rudd v. Briddle, (2019) EWHC 1986 (QB), Para.150 html version of judgement at www.bailii.org (Last visited on November 24, 2019)
[324] Rudd v. Briddle, (2019) EWHC 1986 (QB), Para.154 html version of judgement at www.bailii.org(Last visited on November 24, 2019)
[325] Rudd v. Briddle, (2019) EWHC 1986 (QB) Para. 77-79 html version of judgement at www.bailii.org(Last visited on November 24, 2019)
[326] Rudd v. Briddle, (2019) EWHC 1986 (QB) Para 87-90 html version of judgement at www.bailii.org (Last visited on November 24, 2019)
[327] Rudd v. Briddle, (2019) EWHC 1986 (QB) Para.93, 97 html version of judgement at www.bailii.org
[328] Entick v. Carrington (1765) (19 Howells' State Trials 1029) (95 Eng. Rep. 807)
[329] Gee v. Pritchard, 36 Eng. Rep. 670 (1818)
[330] Pope v. Curl (1741), 26 Eng. Rep. 608 (A),

made by Queen were published in a book in Albert (1848)[331]. The government believed that there is no need to protect the right to privacy as other legal provisions are sufficient to give protection for breach of rights.

In some cases, the protection was provided under breach of confidence as in Saltman Engineering Co(1948)[332] where the use of confidential information was protected and in Coco (1969)[333] the test for confidentiality was provided by the court. Disclosure of the personal information was also protected under breach of confidence as in Douglas (2005)[334]. But after enactment of Data Protection Act the protection was provided under the provisions of the Act. The publication of personal information with the photos of the children was protected under Data Protection and Human Rights Act as in Associated Newspaper Ltd (2012).[335] The privacy claim was upheld when information relating to police action was published on BBC in Cliff Richard[336] (2018).

As Briton was a member of European Union, the protection of personal data was provided strongly by the courts instead of protection of privacy in other aspects. In Halliday [337](2013) the credit information of the person was wrongly sent to credit reference agency was held as breach of privacy of personal information or data breach. In Gulati (2015)[338] voice mail messages of the celebrities were accessed and used to get news for media. It was held that it is breach of data privacy. In Lloyd (2018)[339] it was contended that the data is collected by the browser using cookies and it is used by commercial purposes by the service provider. The court held it is a breach of data protection provisions.

Uses of electronic devices for surveillance was challenged in R (Bridges)[340] (2019) when police had used AFR technology to catch suspects from public places. But Court held that use of such technology is valid one. The interpretation of Data Protection Act provisions was done by the court in Rudd

[331] Albert v. Strange, 41 Eng. Rep. 1171 (Ch) (1848)
[332] Saltman Engineering Co. v. Campbell Engineering co. 3 All E.R 413(1948) 65, RPC 203
[333] Coco v. Clark, R.P.C. 41 U.K. (1969),
[334] Douglas v. Hello! , (2005) EWCA Civ. 95
[335] AAA v. Associated Newspapers Ltd. (2013) EWCA, Civ. 554
[336] Cliff Richard v. BBC (2018). EWHC 1837 (Ch.)
[337] Halliday v. Creation Consumer Finance Ltd. (2013)EWCA Civ. 333(2013)
[338] Gulati v. MGN Ltd. (2015) EWHC 1482 (Ch)
[339] Lloyd v. Google Inc. (2019) EWCA, Civ. 1599
[340] R. (Bridges) v. Chief Constable of South Wales Police and Ors. (2019) EWHC 2341 (Admin)

(2019)[341] where the court has to decide whether the person controlling the site be considered as controller under the Data Protection Act and his responsibility under the Act. It was held that the person operating the site and has decision making power regarding publishing the mater on the site is 'controller' and he was held responsible for publishing defamatory information.

It can be experiential that Briton though does not recognise the 'tort of privacy' as described by Prosser, but provided the protection under tort laws and law regarding breach of confidence. But slowly after Directive 95/46 and GDPR in 2016, for data protection by European Union, the Data Protection Acts are enacted in 1998 and 2018 as Briton was a member of European Union and the privacy claims were decided by the courts on the basis of Data Privacy provisions in those Acts. So today the privacy of personal data or information is emphasized by the court as an important aspect of privacy.

5.6 European Union

The member countries of European Union are following the General Data Protection Regulation which prescribes the rules for processing and transfer of personal data of EU citizens inside or outside European Union. Before this Regulation, member countries were following the Directive 95/46. In Europe, protection of the privacy of an individual was and is associated with the protection against unauthorised access and disclosure of personal data. So the member countries are always providing protection relating to privacy in respect of personal data and not on general grounds of right to property or on defamation or breach of confidence. It is also agreed by them that while interpreting the claim for privacy, the provisions of European Convention of Human Rights shall be followed along with other data protection legislations. Citizens of member countries are allowed to challenge the decision of highest court in such country regarding privacy and data protection claims in Court of Justice of European Union (CJEU). On this backdrop, the researcher has discussed the growth and development of right to privacy in European Union in following paragraphs.

[341] Rudd v. Briddle, (2019) EWHC 1986 (QB)

5.6.1 Right to Protection of Data

As it is discussed in **S and Marper**[342]'s case the application was made by the applicants as their action for breach of privacy of personal data was failed in UK. DNA samples and finger prints of the claimants were preserved by the Authorities for unlimited time. Preservation of such samples is provided according to the law applicable in the country. Applicants demanded erasure of this data and filed an action when their request was denied. Court of Appeal rejected their contention and dismissed the appeal. House of Lords also dismissed the petition. Application was made to European Court of Human Right for the breach of rights under Art. 8 and 14 of Convention. European Court considered that whether retention of fingerprints, DNA profiles and cellular samples constitute an interference in their private life under Art. 8 of the Convention.

It is provided in the Art. 8 that the interference shall be a. in accordance with the law, b. in pursuit of legitimate aim, c. necessary in democratic society. Court has verified the facts on these parameters. Court considered power to retain evidences under s. 64 of Police and Evidence Act, 1984 and compared with legal provisions in other member countries like Scotland, North Ireland and other European Union States. It was of the opinion that it is necessary to distinguish between taking, usage and storage of fingerprints, and sample and profiling is to be justified for its retention. It came to conclusion that "from DNA samples ethnic origin of person can be traced and it is therefore very sensitive data as possibility of affecting personal rights increased. So retention of cellular samples and DNA profiles discloses an interference of applicant's right to respect for their personal life and within the meaning of Art. 8 of the Convention."[343] The court opined that all state collect and retain such data for prevention and detection of crime, but they set certain minimum limit and conditions for retention. "Whether such retention is proportionate and striking fair balance between competing public and private rights is the question to be decided. The court find that blanket and indiscriminate nature of powers of

[342] S and Marper v. UK (2008) ECHR 1581 (application no. 30562/04, 30566/04)
[343] S and Marper v. UK (2008) ECHR 1581 Para. 76, 77 at https://eur-lex.europa.eu/ (Last visited on November 24, 2019)

retention of fingerprints, cellular saple and DNA profiles of persons suspected but not convicted of the offences, as applied in the case of the applicant, fails to strike a fair balance between competing public and private interest and respondent state has overstepped any respectable margin of appreciation in this. It constitutes disproportionate interference with applicant's right to respect private life and cannot be regarded as necessary in democratic society."[344] The court held in favour of the applicants.

5.6.1.1 Freedom of Movement of Data on Internet

In Swedish case, **Bodil Lindqvist**[345] for the first time the scope of Directive 95/46 and freedom of movement of such data on internet was discussed. In this case, Mrs. Lindqvist had set up internet pages on her personal computer to enable parishioners to obtain information which they were likely to need. The information on those pages included first and full names of herself and her 18 colleagues, the description of the work done by them and their hobbies, family backgrounds, telephone numbers and about the foot injury of one of her colleague also. This was challenged.

Mrs. Lindqvist was fined for processing of personal data by automatic means without Datainspektion (Swedish authority for protection of electronically transmitted data), for transferring data to third countries without authority and for processing sensitive personal data (foot injury of a colleague). She appealed against the decision. The case was referred to Court of Justice European Commission (CJEC) for consideration that whether activities of Mrs. Lindqvist are contrary to provisions of Data Protection Directive 95/46.

Court had held that act of referring on internet page, to various persons and identifying them by name or other constitutes 'processing of personal data wholly or partly by automatic means'.[346] Moreover reference to state of health of an individual amounts to processing of data concerning health within the

[344] S and Marper v. UK (2008) ECHR 1581. Para.125 at https://eur-lex.europa.eu/ (Last visited on November 24, 2019)
[345] Bodil Linqvist v. Aklagarkammaren I Jonkoping (2003), C-101/01, ECLI:EU:C:2003:596, Retrieved from https://curia.europa.eu/en. (Last visited on November 24, 2019)
[346] Bodil Linqvist v. Aklagarkammaren I Jonkoping (2003)Para.27 at https://curia.europa.eu/en (Last visited on November 24, 2019)

meaning of Directive.[347] Directive points out certain rules for monitoring the transfer of personal data to third countries.[348] The appeal was dismissed.

5.6.1.2 Health Data and Right to Privacy

The issue of health data protection was raised by an applicant in **V v. Parliament (2011)**,[349] for medical examination for appointment as staff. The fitness in medical examination was a precondition for the appointment. His appointment was cancelled by European Parliament after the medical examination was done. The issue was raised by the applicant that transfer of medical data between the institutions is breach of protection of privacy because of processing of it under Art. 8-Right to respect for private life. The Civil Service Tribunal held that it is breach of protection of privacy. It annulled the withdrawal of offer made to V. It had ordered European Parliament to pay EUR 25000 to V. It also ordered European Parliament to withdraw the annulment order of employment made to V.

5.6.1.3 Cross Border Data Transfer and Right to Privacy

European Union data rules prohibit the transfer of personal data outside the Union by default. The transfer is permitted only if the other country to which the personal data is transferred is providing adequate data protection. European Union Directive is providing the norms for such protection. Directive also provides that European Commission may find that the third country ensures the protection. If the Commission arrives to such decision, the data can be transferred to such country. In July, 2000, European Commission has decided that United States is providing adequate safeguards to data protection. The decision was based on Safe Harbour Principles for transferring the data in which American companies voluntarily subscribe for the cross-border data transfer.

Any person residing in European Union who wishes to use Facebook is required to enter in to contract, at the time of his registration, with Facebook Ireland, a

[347] Bodil Linqvist v. Aklagarkammaren I Jonkoping (2003)Para.51 at https://curia.europa.eu/en (Last visited on November 24, 2019)
[348] Bodil Linqvist v. Aklagarkammaren I Jonkoping (2003)Para. 63-66 at https://curia.europa.eu/en (Last visited on November 24, 2019)
[349] V v. Parliament, F-46/09(Staff case-2011/C/282/92) (2011). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=oj:c:2011:282 . (Last visited on November 24, 2019)

subsidiary of Facebook Inc. which itself if established in United States. Some or all of the personal data of Facebook Ireland users who reside in European Union is transferred to servers belonging to Facebook Inc. that are located in United States, where it undergoes processing. But after the revelation by Edward Snowden, **Max Schrems**,[350] an Austrian, privacy activist and Facebook user, filed complaint with Irish Data Protection Commission. He asked the Commissioner to prohibit Irish subsidiary (Facebook-Ireland) to transfer his personal data to the servers based in America (Facebook-Inc.) He contended that according to revelation by Snowden, USA did not adequately protect personal data from National Security Agency (NSA) surveillance activities.

The Irish authority refused to investigate the complaint on the ground that in 2000, European Commission had decided that USA is providing adequate privacy protection by its decision 2000/520.

Schrems then challenged the decision before Ireland's High Court. High court of Ireland noted that many US agencies carried out surveillance of personal data which is in contrary to Irish privacy law. It recognised that Schrems is validly challenging the decision 2000/520 and safe harbour framework. It stayed the case and referred the question to CJEU that whether the national data protection authority could investigate the adequacy of data protection of third country independently or the Commissioner is totally bound by the decision of the European Commission.

Court of Justice answered the question in affirmative and held that national supervisory authority can examine the adequacy of data protection that whether it complies with requirements laid down in EU Data Protection Directive.[351] It also held that safe harbour principles did not adequately protect personal data from interference from US Government. So the decision 2000/50 was declared invalid. [352]

[350] Max Schrems v. Data Protection Commissioner (2015) ECLI:EU:C:2015:650
[351] Max Schrems v. Data Protection Commissioner (2015) ECLI:EU:C:2015:650. Para 66, 107 at https://eur-lex.europa.eu (Last visited on November 24, 2019)
[352] Max Schrems v. Data Protection Commissioner (2015) ECLI:EU:C:2015:650. Para. 107 at https://eur-lex.europa.eu (Last visited on November 24, 2019)

5.6.2 Photographs and Right to Privacy

In **Von Hannovar v. Germany (2004)**[353], the applicant, Princess Caroline, belongs to Royal Family of Monaco. The applicant made an application for injunction regarding publication of her photographs published in German magazine Bunte and Renzeit Revue. She has submitted that because of the publication of photos her right to protect her personal life is breached. There were three series of photos.

In 1993, an applicant sought injunction in Hamburg Regional Court against further publication on the ground that they infringe her right to protection of her personality rights and her right to protection of her private life and to control of use of her image under Copyright Act. Injunction was granted with regard to distribution in France in accordance with private international law. But with regard to distribution in Germany, German law applies and it expressed the opinion that applicant being a public figure "par excellence" has to bear such publishing.

Court of Appeal, 1994, had vacated the injunction and dismissed the application. Federal court of Justice, in 1995, allowed the appeal in part, granting injunction against further publication of photos that had appeared in Freizeit Revue. But it rejected remainder of appeal holding that applicant being a public figure "par excellence" has to bear such publishing. Public has legitimate interest in knowing where applicant was staying and how she behaved in public.

Federal Constitutional Court of Germany, in 1999, allowed it in apart on the ground that three photos published in Bunte magazine applicant with her children had infringed her right to protection of her personality rights. It dismissed the appeal with regard to other photos. The Applicant reapplied to restrain publishing of second and third series of photos in all the above courts according to their hierarchy. The Courts in these reapplications refused to grant relief and dismissed the appeal. The last decision regarding publication of photos especially showing the applicant tripping over the obstacle at Monte Carlo Beach Club, the Constitutional Court of Germany refused to grant an

[353] Von Hannovar v. Germany (2004) ECHR 294

injunction restraining the publication of photographs and held that "ordinary courts had properly found that Monte Carlo Beach Club was not secluded place and that the photos of applicant wearing swimming suit and falling down were not capable of constituting an infringement of her right to respect her private life"[354].

The application was made to Court of Justice of European Union. She had submitted that "under German law, protection to private life of public figure is minimal because of the concept of 'secluded place' is very narrow as defined by Federal Constitutional court. Further, the onus is put on her every time to prove that she was in secluded place-private place. The photos are not published for information, but only for entertainment of the people"[355].

The German Government argued that "the publication of photos and information about elite people is covered under freedom of press. The laws have sufficient safeguards for protection of personal life of public figure and prevent any abuse. Government had struck correct balance between Art. 8-protection of privacy and Art. 10 freedom of press."[356]

Court of Justice reiterated the principle which it had held in many cases that "concept of private life extends to aspects relating to personal identity, person's name or person's picture, his physical psychological integrity"[357]. The court considered that "the decisive factor in balancing the protection of private life against the freedom of expression should lie in contribution that the published photos and article make to a debate of general interest. It is clear in instant case that there is not such contribution since the applicant has not exercised no official function and the photos and articles related exclusively to detail of her private life. It was held that the publication of photos was the breach of privacy

[354] Von Hannovar v. Germany (2004) ECHR 294Para. 38, html version of judgement at www.bailii.org (Last visited on November 21, 2019)
[355] Von Hannovar v. Germany (2004) ECHR 294Para. 44. html version of judgement at www.bailii.org (Last visited on November 21, 2019)
[356] Von Hannovar v. Germany (2004) ECHR 294Para. 45 html version of judgement at www.bailii.org (Last visited on November 21, 2019)
[357] Von Hannovar v. Germany (2004) ECHR 294 para. 50 html version of judgement at www.bailii.org (Last visited on November 21, 2019)

under Art. 8 of the Convention.[358] Every one including celebrities has right of 'legitimate expectation' that his private life shall be protected."

5.6.3 Right to be Forgotten

One of the important rights to data subject which was provided in the Directive was 'Right to be forgotten'. It means the data subject can ask to erase inaccurate or irrelevant information about him which is collected and stored by the controller. In **Google v. Spain (2010)**[359], the CJEU discussed the conditions to be satisfied for exercise of this right validly. A resident of Spain Mr. Costeja Gonzalez lodged a complaint with AEPD (Spanish Data Protection Authority) against the newspaper 'La Vanguardia' and against Google Spain and Google Inc.

The complaint was based on the fact that when any user entered the name 'Mr. Gonzalez' in 'Google search', two links are opening showing the news published in 'Vanguardia' of 19th January and 9th March 1998-where announcement is published mentioning Mr. Gonzalez name for auction of his immovable property for recovery of social security debts. [360]

Mr. Costeja Gonzalez requested two things, that La Vangaurdia required either to remove/alter the pages so that his personal data no longer appear on search engine and Google Spain or Google Inc. be required to remove or conceal personal data relating to him-so that will not include in search result and no longer appear in links to 'La Vanguardia'. Mr. Gonzalez stated that attachment proceedings concerning him had been fully resolved for number of years and reference to them was not relevant now.[361]

In July 2010, AEPD rejected the complaint in terms of 'La Vanguardia' holding that publication of the information is legally justified as it was published on order of Ministry of Labour and Social Affairs. Complaint against Google was upheld holding that operators of search engine are subject to data protection legislation. They carry out data processing and act as intermediary. When

[358] Von Hannovar v. Germany (2004) ECHR 294Para. 76-81 html version of judgement at www.bailii.org (Last visited on November 21, 2019)
[359] Google v. Spain (2010) C-131/12
[360] Google v. Spain (2010) C-131/12 Para. 14 at https://eur-lex.europa.eu/ (Last visited on November 21, 2019)
[361] Google v. Spain (2010) C-131/12 Para. 15 at https://eur-lex.europa.eu/ (Last visited on November 21, 2019)

fundamental right of data protection and dignity is breached by locating and disseminating a data by search engine, Data Protection Authority has power to withdraw and prohibit this. [362]

Google Spain and Google Inc. challenged this decision separately before National High Court which had joined the actions. The reference was made to EU Court. The issues in this case were- 1. Whether providing the content by the search engine is 'processing of data' as per definition in Art. 2 (b) of Directive 95/46. It was argued by Google that it has no control over the content uploaded by third parties. 'Content' includes providing information which is published/ placed on internet by 3rd parties indexing it automatically, storing it temporarily and making available to internet users.

Court held that "uploading of data is included in processing of data. Third parties are exploring the internet automatically, constantly and systematically in search of information, which is published by operator of search engine, collects such data, subsequently 'retrieves', 'records' and organises within framework of indexing program, 'stores, on its servers and 'discloses' and 'makes available' to its users. These operations are included in definitions of processing in Art. 2(b) of Directive."[363]

2. Whether search engine is 'Controller'? Art. 2 (d) of the Directive- "Controller is natural person or legal person, public authority agency or any other body which alone or jointly with others determines the purpose and means of processing of personal data. Search engine operator which determines the purpose and means of that activity and thus of processing of personal data that it itself carries and within framework of that activity and which must, consequently be regarded as 'controller' in respect of processing. Activity of search engines play decisive role in overall dissemination of those data by making is available to any internet user who wants to search. Otherwise user would not be also to find webpage the information. Search engine facilitate the user to access information by name, giving detailed information of the person.

[362] Google v. Spain (2010) C-131/12 Para. 16-17 at https://eur-lex.europa.eu/ (Last visited on November 21, 2019)
[363] Google v. Spain (2010) C-131/12, Para. 30-31 at https://eur-lex.europa.eu/(Last visited on November 21, 2019)

It gives profile of data subject. So operator shall be regarded as 'controller' in respect of that processing, within the meaning of Art. 2(d). He shall ensure the fundamental right to privacy.[364]

3. Whether data subject requires the operator of search engine to remove data which is true on the ground that it may be prejudicial to him or that he wishes to be forgotten after sometime. "Art. 6 (1) (a) to (e) provides collected personal data become incompatible as no longer necessary with lapse of time though initially it was lawfully processed, the data subject can request to controller to remove it under Art. 12 (b). [365] It was also clarified by the court that "right of data subject to remove the information must override the economic interests of operator and interest of general public in finding that information upon data subject's name."[366] It was also held that, "Here as the sensitivity of the information about data subject regarding recovery of debt through auction, and the information of data subject's private life contained in these announcements and to fact that initial publication had taken place 16 years earlier, data subject had established the right that the information shall not be linked to his name by such list."[367]

The same issue was raised again in **Google v. CNIL**[368] (French Data Protection Authority). The CNIL issued the notice to Google that while acting on the request to de-reference the search results, company must apply the removal globally rather than just the domain of requester's residence. The Company refused on the ground that it will be taken advantage by authoritarian governments. Google was ready to use 'geo blocking technique' that would prevent a user in European Union States from accessing links de-referenced in European Union. CNIL found it inadequate and imposed fine. Google appealed to Conseil for annulment of this decision. Conseil referred it to the Court of Justice of European Union (CJEU).

[364] Google v. Spain (2010) C-131/12, Para. 32-38 at https://eur-lex.europa.eu/ (Last visited on November 21, 2019)
[365] Google v. Spain (2010) C-131/12, Para. 94 at https://eur-lex.europa.eu/ (Last visited on November 21, 2019)
[366] Google v. Spain (2010) C-131/12, Para. 97 at https://eur-lex.europa.eu/(Last visited on November 21, 2019)
[367] Google v. Spain (2010) C-131/12, Para 98 at https://eur-lex.europa.eu/ (Last visited on November 21, 2019)
[368] Google v. CNIL, C-507/17, EUR-Lex CELEX NO 62017CJ0507 (Sept. 24-2019).

The Court verified the Data Protection Directive 1995 and General Data Protection Regulation, 2016. It had held "that there is a right to protect personal data throughout European Union but it is not absolute. It is to be balanced with the rights of other parties of having access to information in accordance with principles of proportionality"[369]. "Where a search engine operator grants a request for de-referencing pursuant to the provisions, is not required to carry out de-referencing on all versions of its search engine, but on version of search engine corresponding to all member states while taking necessary measures."[370]

5.6.4 Discussion

European Union was and is vigilant about the invasion and breach of privacy from period when information technology was used by technologically developed countries only. The OECD principles of privacy in 1981 had sensitized the world about invasion and breach of data/information. Data protection directive 95/46 and General Data Protection Regulation in 2016 are the steps taken by the Union which provide guideline for many countries who are lacking any type of legislation for protection of information or data.

It is evident from the cases discussed so far that the violation or encroachment on privacy was done by government through exercising powers of search and seizure, and by journalists of print and electronic media by publishing the personal information publicly, this encroachment is controlled by the courts. Courts tried to give protection under property laws and tort laws. The cases which could not be covered under property laws or tort laws, they were protected by applying guarantees given in Bill of Rights as in USA or by applying fundamental rights provisions as in India. The Courts in UK tried to protect this right on the grounds of property torts earlier and then applying Human Rights legislation.

It is evident that 'Right to Privacy' has developed as encroachment on private life has increased due to advent of technology. Every society sanctifies domestic

[369] Google v. CNIL, C-507/17, EUR-Lex CELEX NO 62017CJ0507. Para 60 at https://curia.europa.eu/ (Last visited on November 21, 2019)
[370] Google v. CNIL, C-507/17, EUR-Lex CELEX NO 62017CJ0507. Para. 74 at https://curia.europa.eu/ (Last visited on November 21, 2019)

life, so this right was recognised as 'right to be let alone'[371]. As scope of legal rights broadened, the new contours of 'Right to Privacy' emerged. With development of information technology and computers, chances of disclosure of the personal information or data have increased. So now courts are focusing more on informational privacy and data protection, e.g. attaching the GPS system without warrant to the vehicle of accused to collect data for his activities amounts to 'search' and therefore invalid as held by USA Court.

On electronic media, whichever the activity is done is permanently stored in the memory of computer and on cyber space. The information which is published in cyber space is circulated worldwide and permanently available on the click of the button. This way any matter related to an individual which had happened in the past can also have a chance to smear the future of him. The European Union has provided the unique provision under the General Data Protection Regulation (GDPR) relating to right to be forgotten. Under this provision, if the matter earlier published on cyber space has become irrelevant or if its purpose is served, the data controller, if the request is made by data principal or data subject, shall remove it from the cyber space. Every person shall have a second chance to correct himself. Because of this provision, it has become possible that on the basis of the matter published earlier relating to his transactions, he should not be judged relating to his current or future transactions.

The second unique feature of the European Union's data protection regime is that it provides that cross border transfer of data is only permissible if the other country has equally strong data protection legislation in its legal system. For this equal protection purpose, decision taken by European Commission is final. Accordingly, in July, 2000, European Commission has decided that United States is providing adequate safeguards to data protection and Safe Harbour principles were provided for such transfer. American companies voluntarily subscribe for the cross-border data transfer. But after the revelation by Edward Snowden, **Max Schrems**,[372] an Austrian, privacy activist and Facebook user, filed complaint with Irish Data Protection Commission. In this case it was held that safe harbour principles did not adequately protect personal data from

[371] Warren and Brandeis, "The Right to Privacy", Harvard Law Review (1890), Vol.4, No.5 pg, 193
[372] Max Schrems v. Data Protection Commissioner (2015) ECLI:EU:C:2015:650

interference from United States Government. So the decision 2000/50 was declared invalid. [373] After that the Privacy Shield Framework protection agreement was entered into and now the transactions are governed under Privacy Shield Framework.

5.7 Judicial Trends in Right to Privacy: Comparative Analysis

From the above, it can be seen that in United States the courts were providing protection for the Right to Privacy from the late 19th Century. Courts have the great contribution for shaping the opinion of society and creating awareness about Right to Privacy in United States of America. The courts in United States expanded the concept 'privacy' to its maximum by providing the criteria 'reasonable expectation of privacy'.

In English legal system, this right was never recognised as separate and specific right. Courts in England used to term this right as 'tort of privacy' and protected it under law of Torts. For disclosure of information, courts provided protection under breach of confidence. The situation has changed relating to personal data only after the Data Protection Acts were enacted being a part of European Union.

In European Union, privacy was and is related to the personal information or personal data. Therefore, from the beginning, the emphasis was given for protection of personal information or data by the courts. Accordingly, the Data Protection Privacy principles were provided for the data privacy. And as the need has arisen to protect data more strongly because of increased use of information technology in processing of data, the General Data Protection Regulation was enacted and decisions are given on the basis of these provisions by the courts. European Union Courts were one of the firsts to recognise the right to be forgotten.

Judiciary in India was and is protecting this Right to Privacy under fundamental right to life and liberty under Art. 21 of Constitution of India. There was no legislation for protection of Right to Privacy. Information Technology Act, 2000 was enacted which provides insufficient protection for Right to Privacy.

[373] Max Schrems v. Data Protection Commissioner (2015) ECLI:EU:C:2015:650. Para. 107 at https://eur-lex.europa.eu (Last visited on November 21, 2019)

Therefore, Courts are protecting this right under Art. 21. Courts have decided the matters based on the provisions of Information Technology Act, 2000 relating to responsibility of intermediaries mostly.

The judicial trend in all the countries under study has been evolving and responding to the technological advancements of the day. Right of legitimate expectation has been upheld in the context of protection of privacy in all the countries under study. A paradigm shift in the approach of the judiciary is seen while dealing with the aspects of informational or data privacy. The technological developments had thrown challenge to the basic human rights of freedom of speech and expression and right to life. By giving a broad interpretation in consonance with prevailing Constitutions, it has been found that the Court have applied the existing provisions to the issues arising out of scientific or technological developments in the absence of any specific legisations at times.

Protection of Privacy rights under Information Technology Act, 2000 have not arisen before the Indian Courts. Issues like erasure of the data, or cross border transfer of data have not yet arisen before the Indian Courts till date, hence the approach of the Judiciary in this regard is not yet known. These issues have arisen in the European Union etc, wherein the Courts recognised the Right to be Forgotten and later it led to the drafting of GDPR which has been extensively dealt by the Researcher in Chapter Three.

After discussing the Judicial Approach in protection of right to Privacy, the researcher shall study, discuss and analyse the opinion of the various stakeholders in the next Chapter.