CHAPTER 4
INTERNATIONAL PERSPECTIVE

4.1 Introduction

The researcher submits that it is only after two world wars, the whole world got enlightened with the idea of Human Rights. Every civilized State wanted to create a peaceful world. Consequently, interaction amongst these states increased and the basic nomenclature of international law was founded. At the international level, the international body was established in the name of “United Nations” to achieve and promote the peace and justice. At the time of its establishment, United Nations was very well acquainted with the fact that the standard of basic human rights was at the worst stage. In order to increase the standard of human rights, many declaration and conventions were made at international level and state parties were held responsible to follow these conventions and declarations. Although privacy concerns are deeply rooted in history, privacy protection as a public policy question can be regarded as a comparatively modern notion. The right to privacy has, however become one of the most important human rights of the modern age and is today recognised around the world in diverse regions and cultures.\(^1\)

4.2 International Instruments protecting Right to Privacy

The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights, which specifically protects territorial and communications privacy. Article 12 of the Universal Declaration of Human Rights (1948) protects individuals’ privacy, honour and reputation, their families, home, and correspondence against any arbitrary interference.\(^1\) Article 17 of the International Covenant of Civil and Political Rights\(^2\) (to which India is a party), contains the same wordings and protects everybody’s privacy.

---

1. http://old.ispa.org.za/regcom/privacyfiles/chapter-2-rigthtoprivacy.pdf accessed on July 1, 2012 at 8:00 a.m IST.
   It provides as follows:
   “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

3. The International Covenant of Civil and Political Rights, Art. 17.
   It provides as follows:
   “1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
   2. Everyone has the right to the protection of the law against such interference or attacks.”
The right to privacy is also dealt with in various other international instruments, such as the United Nations Convention on the Rights of the Child, the International Covenant on Civil and Political Rights (ICCPR), and the United Nations Convention on Migrant Workers. For example, The United Nations Convention on the Rights of the Child, which was adopted on 20 November 1989, and entered into force on 2 September 1990, speaks through Article 16. It protects children’s privacy, honour and reputation.4

Furthermore, Article 8 of the European Convention on Human Rights, which came into effect on Sept. 3, 1953, while respecting one’s private and family life, allows public authority’s interference only under exceptional circumstances. It represents that right to privacy is not absolute right and, the public authority can interfere one’s private life in the interests of national security and public safety. Moreover, privacy rights are not available by jeopardizing others’ health, morals, rights, and freedoms.5

The European Court of Human Rights in Strasbourg has dealt with many complaints from individuals seeking remedies against the violation of their privacy rights under Article 8 of the European Convention on Human Rights. While dealing with the individual complaints, the court found many shortcomings in the domestic law of several European jurisdictions. For example, in Gaskin v. United Kingdom,6 following the death of his mother, the applicant was received into care by a local authority. He ceased to be in the care on attaining the age of majority. In the period during which the applicant was in care, he was boarded out with various foster parents.7 He contends that he was ill-treated.8 The applicant, wishing to bring proceedings against the local authority for damages for negligence, made an application for discovery of the

---

4 United Nations Convention on the Rights of the Child, 1989, Art. 16. It provides as follows:
1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
2. The child has the right to the protection of the law against such interference or attacks.”
5 The European Convention on Human Rights, Art. 8. It provides as follows:
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals or for the protection of the rights and freedoms of others.”
6 Application no. 10454/83, Judgment from the European Court of Human Rights, Strasbourg, 7 July 1989. Available at http://hudoe.oechr.coe.int/sites/eng/pages/search.aspx?i=001-57491#itemid:"001-57491"} accessed on July 20, 2013, at 4:00 p.m. IST.
7 Id., paragraph 10.
8 Id., paragraph 11.
local authority's case records made during his period in care. Discovery was refused by the High Court on the ground that these records were private and confidential. 

Finally, the European Court opined that persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development. 

Furthermore, the Canadian Charter of Rights and Freedoms recognizes everyone’s right to life, liberty and security. It also provides that everyone has the right to be secure against unreasonable search and seizure. Similarly, the New Zealand Bill of Rights declares in section 21 that everyone has the right to be secure against unreasonable search or seizure, whether of the person, property or correspondence or otherwise.

4.3 European Union and Data Privacy

At the International level, the first serious concern regarding data protection took place in the year of 1968 when United Nations International Conference on Human Rights was held. The first data protection statute was enacted in German State of Hesse in 1970. Thereafter, in 1973, Sweden also adopted its first national statute on data protection. Since then the ‘Fair information practices’ (FIPs) have been recognized as basic principles for the protection of Data privacy in many countries. Fair Information practices are a set of principles for defining and addressing concerns about privacy of personal information. However, Fair information practices

---

9 Id., paragraph 14.
10 Id., paragraph 49.
11 Canadian Charter of Rights and Freedoms, Section 7. Available at http://laws-lois.justice.gc.ca/eng/Const/page-15.html/#bh-44 accessed on July 20, 2013, at 4:00 p.m. IST. It provides as follows:
“Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.”

12 Id., Section 8. It provides as follows:
“Everyone has the right to be secure against unreasonable search or seizure.”

13 New Zealand Bill of Rights Act 1990, Section 21. Available at http://legislation.govt.nz/act/public/1990/0109/latest/whole.html#DLM225523 accessed on July 20, 2013, at 4:00 p.m. IST. It provides as follows:
“Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.”

were invented by a United States government advisory committee in a 1973 report in response to the growing use of automated data systems containing information about individuals. The committee found that under prevailing law (at that time in 1973), a person’s privacy is poorly protected against arbitrary or abusive record-keeping practices. For this reason, as well as because of the need to establish standards of record-keeping practice appropriate to the computer age, the committee’s report recommended the enactment of a Federal ‘Code of Fair Information Practice’ for all automated personal data systems. The Committee’s original formulation of the Code was:

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

To implement such principles, United States passed Privacy Act of 1974. Subsequently, with the rise in the information technology and computerized data processing, in 1980, the Organisation for Economic Co-operation and Development (OECD) decided, in 1980, recommended Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the “Privacy Guidelines”). By setting out core principles, the guidelines play a major role in assisting

---

17 http://epic.org/privacy/hew1973report/Summary.htm accessed on July 20, 2013, at 4:00 p.m. IST
18 ibid.
governments, business and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to transborder data flows, both on and offline.¹⁹

4.3.1 Organization for Economic Cooperation and Development

On 11 April 1985, Organization for Economic Cooperation and Development (OECD) Ministers adopted the Declaration on Transborder Data Flows. This Declaration addressed the policy issues arising from flows of personal data across national borders, e.g. flows of data and information related to trading activities, intra corporate flows, computerised information services, and scientific and technological exchanges. The eight principles set out by the Organization for Economic Cooperation and Development (OECD) are:²⁰

(a) Collection Limitation Principle: Personal data should be collected in a very limited manner. Indeed, while collecting personal data, lawful and fair means should be adopted. In appropriate cases, it should be obtained with the knowledge and consent of the data subject.

(b) Data Quality Principle: It is necessary that Personal data should be relevant to the intended purposes and, should be accurate, complete and kept up-to-date.

(c) Purpose Specification Principle: At the time of data collection, purpose should be specified and should be used for that purpose only.

(d) Use Limitation Principle: The consent of the data subject or the authority of law is required to disclose the personal data. Same consent or authority is necessary if the data is used for unintended purposes.

(e) Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

(f) Openness Principle: It is required that an individual should have a way to know the existence, nature, and, purposes of personal data. There should also be a certain means to


know the identity and residence of the data controller. In other words, there must be openness in developments, practices and policies of collecting the personal data.

(g) **Individual Participation Principle:** An individual should have the right to confirm that whether a data controller has data relating to him or not. Such confirmation should be communicated to him within reasonable time and in reasonable manner. If the data controller denied the request, then it becomes necessary on his part to give reasons for such denial. Furthermore, the individual should have the right to challenge the denial. Besides, the individual should have the right to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

(h) **Accountability Principle:** Under this principle, a data controller should adopt certain measures to give effect to the above said principles.

Therefore, it has been observed that European Union Directive also adopted the ‘fair information practices.

### 4.3.2 European Data Protection Directive 1995

However, the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (the Directive) has been considered as backbone of European Union (EU) data privacy protection laws. The Directive of 1995 was laid down for the protection of individuals with regard to the processing of personal data and on the free movement of such data. The motive of the Directive was to develop economic growth, while protecting European Union’s citizens’ privacy.\(^{21}\) It was intended that there should be a free flow of personal data within European Union member countries, while affording the privacy protections to the citizens. Even if data is being transferred outside of European Union (EU) member countries, protection should be given to such data. Furthermore, personal data is barred from transferring to a third country who doesn’t have an adequate law on privacy protections.\(^{22}\) For example, a business traveler from a country without adequate protection may not take data about business or customer contacts collected in European Union (EU) member countries outside the European Union (EU). By barring the transfer of personal data from European Union (EU) citizens to businesses and

---


other entities in countries without levels of privacy protection deemed appropriate by the European Union (EU), the directive sets de facto standards for data protection internationally. Accordingly, countries such as Canada, Australia, and Japan have implemented data protection laws that provide similar levels of protection for personal data. Others—in particular the United States—have worked out special agreements with the European Union (EU) so that U.S. businesses can claim compliance with these principles.23

The Directive considered the right of individuals to control the collection, distribution, and use of their personal information as a traditional human right, which can be protected only by implementing ‘fair information practices’ i.e. principles of openness, access and correction, collection limitation and finality, accuracy, security, and enforcement or redress.24

The Directive prohibits European Union (EU) member states from collecting data that reveal an individual’s ethnic origin, race, political conviction, religious beliefs, or health and sexuality.25 However, an authorized entity has the right to collect such type of data.

4.3.3 European Commission’s Communication, 2010

In 2010, European Commission’s Communication entitled, “A comprehensive approach on personal data protection in the European Union,” revised the existing European Union (EU) data protection directives to check its validity in the technological world. It was stated that Directive of 1995 is a historical document in the field of data protection in the European Union. It was born with two objectives i.e. the protection of personal data, on the one hand, and the free flow of personal data for economic growth, on the other. After conducting thorough research, it was concluded by the Commission that the objectives and the principles enshrined in the Directive remain valid.26

However, the European Commission noticed that due to advancement in rapid technological developments and globalization have brought new challenges for the protection of personal data. The commission observed that technology and social networking sites has made easy for individuals to share personal information publicly and globally. This sharing of personal

---

24 Id., at 208.
25 Art. 8(1) of Directive 95/46/EC. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML accessed on April 22, 2012, at 12:00 p.m. IST.
information leads to ‘Cloud computing’, which is being considered as a serious challenge to data protection. In such phenomenon, the individual loses control over his sensitive information.\textsuperscript{27}

Similarly, sophisticated technologies and automatic data processing systems have made easy to determine individuals’ location. The economic operators are using sophisticated tools for target marketing. At the same time, Public authorities use personal data for various purposes, such as tracing individuals in the event of an outbreak of a communicable disease, for preventing and fighting terrorism and crime more effectively, to administer social security schemes or for taxation purposes, as part of their e-government applications etc.\textsuperscript{28}

Therefore, by considering these challenges, the Commission reviewed the existing European Union (EU) data protection legislation. After public consultation, the Commission validated the core principles of the Directive are still valid and, held that its technologically neutral character should be preserved. However, during public consultation, several problems were identified which are as follows:\textsuperscript{29}

\begin{itemize}
  \item **Impact of new technologies:** People really wanted that data protection principles should be updated with new technologies.
  \item **Enhancing the internal market dimension of data protection:** In spite of a common European Union (EU) legal framework, there is the lack of sufficient harmonisation between Member States' legislation on data protection.
  \item **Addressing globalisation and improving international data transfers:** Stakeholders highlighted that Law is not clear regarding increased outsourcing of processing. Current schemes are not satisfactory with respect to international data transfers.
  \item **Providing a stronger institutional arrangement for the effective enforcement of data protection rule:** Role of Data Protection Authorities needs to be strengthened so as to ensure better enforcement of data protection rules.
  \item **Improving the coherence of the data protection legal framework:** Every stakeholder wanted an overarching instrument applying to data processing operations in all sectors and policies of the Union, ensuring an integrated approach as well as seamless, consistent and effective protection.
\end{itemize}

While considering the impact of globalisation and new technologies, therefore, the Commission endeavoured to modernise the European Union (EU) legal system for the protection

\textsuperscript{27} Ibid.
\textsuperscript{28} Ibid
\textsuperscript{29} Id. at 3.
of personal data in all areas of the Union’s activities. In order to make an effective legislation the Commission decided to consider and examine the ways to implement following objectives:\footnote{Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final - 2012/0011 (COD). Available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexpliis!prod!CELEXminidoc&lg=en&mmdoc=32012PC0011 accessed on April 22, 2012, at 12:00 p.m. IST. 30}

- Coherent application of data protection rules in technological world.
- Transparency in the processing of personal data and more obligations on data controller.
- Principle of data minimization should be strengthened. Also, improvement in the rights of access, rectification, erasure or blocking of data.
- Clarification in the so-called ‘right to be forgotten’. This right needs clarification because the Commission observed that individuals usually fail to retrieve personal data from social networking sites, such as their pictures.
- Awareness among general public, particularly youngsters.
- Informed and free consent to be strengthened.
- Whether genetic data should be considered as ‘sensitive data’ or not.
- Effective provisions on remedies and sanctions.
- Enhancement in data controllers’ responsibility, such as to carry out a data protection impact assessment in case of sensitive data.
- Encouragement to self-regulatory initiatives.
- Application of the general data protection rules to the areas of police and judicial cooperation in criminal matters. The Commission intends to examine how
- Promoting the development of high legal and technical standards of data protection in third countries and at international level.

Finally, to implement such objectives, the Commission promised to propose legislation in 2011.

Recently, on 25\textsuperscript{th} January 2012, European Commission’s Communication gave a proposal on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Article 1(7) of the proposal provides that high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of
Members States is necessary for effective judicial co-operation in criminal matters and police cooperation. Therefore, in order to achieve this end, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties must be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.\(^31\)

### 4.4 Asia-Pacific Economic Cooperation (APEC)

Asia-Pacific Economic Cooperation (APEC) is the premier Asia-Pacific economic forum whose goal is to support sustainable economic growth and prosperity in the Asia-Pacific region. It is united to build a dynamic and harmonious Asia-Pacific community by championing free and open trade and investment, promoting and accelerating regional economic integration, encouraging economic and technical cooperation, enhancing human security, and facilitating a favorable and sustainable business environment. Forum’s initiatives turn policy goals into concrete results and agreements into tangible benefits.\(^32\)

Asia-Pacific Economic Cooperation (APEC) economies recognize the importance of protecting information privacy and maintaining information flows among economies in the Asia Pacific region and among their trading partners.\(^33\)

After European Union Directives, the Asia-Pacific Economic Cooperation (APEC) economies have adopted the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. Asia-Pacific Economic Cooperation (APEC) Ministers at their November 2004 meeting in Santiago, Chile, announced their endorsement of the Framework, which had been developed over the last two years by Asia-Pacific Economic Cooperation’s (APEC) Electronic Commerce Steering Group (ECSG) Privacy Subgroup. The Asia-Pacific Economic Cooperation (APEC)...

---


32 [http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx](http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx) accessed on April 22, 2012, at 3:30 p.m. IST.

33 [http://www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx) accessed on April 22, 2012, at 3:30 p.m. IST.
Privacy Framework consists of a set of nine ‘Asia-Pacific Economic Cooperation (APEC) Privacy Principles’ in Part III, plus a preamble and scope note in Parts I and II. Asia-Pacific Economic Cooperation (APEC) has been moving slowly toward privacy standards since 1995.34 The first Asia-Pacific Economic Cooperation (APEC) document to consider privacy issues as a matter of regional significance was the Seoul Declaration for the Asia-Pacific Information Infrastructure(APII) made at the Senior Officials Meeting on Telecommunications and Information Industry, held in 1995 in Seoul, which included privacy in its ‘ten core principles’ but otherwise said little. The 3rd Asia-Pacific Economic Cooperation (APEC) Ministerial Meeting on the Telecommunications and Information Industry in 1998 made a Singapore Declaration stressing the importance of electronic commerce to Asia-Pacific Economic Cooperation (APEC), and included privacy as an issue to be considered in relation to consumer confidence in e-commerce. However, there was no specialist Asia-Pacific Economic Cooperation (APEC) group to deal with privacy issues until the 1999 establishment of the Asia-Pacific Economic Cooperation Electronic Commerce Steering Group (APEC ECSR) by the Asia-Pacific Economic Cooperation (APEC) Senior Officials meeting in Wellington, New Zealand. The Privacy Subgroup was then established and held a ‘mapping exercise’ of regional privacy laws in 2002. Asia-Pacific Economic Cooperation (APEC) then moved to develop a regional privacy instrument.35

There have been occasional calls since the mid-90s for an Asia-Pacific privacy standard to be developed from Asia-Pacific Economic Cooperation (APEC) structures, and from the distinctive regional form that privacy laws have taken in the Asia-Pacific, described by Waters as ‘a third way in data protection’.36 Europe has successfully developed binding regional instruments in the field of data protection with both the Council of Europe Convention of 1981 and the Directive of 1995. It would be a logical and valuable development for the Asia-Pacific, the second region in the world to develop a concentration of privacy laws, to also develop a distinctive regional Convention on data protection. It was not until late 2002 that a number of

---

Asia-Pacific Economic Cooperation (APEC) economies started to move Asia-Pacific Economic Cooperation (APEC) processes in the direction of a regional privacy agreement. At a meeting of the Asia-Pacific Economic Cooperation Electronic Commerce Steering Group (APEC ECSG) in Thailand in February 2003, Australia put forward a proposal for the development of Asia-Pacific Economic Cooperation (APEC) privacy principles using the Organization for Economic Cooperation and Development (OECD) privacy principles as a starting point, plus implementation mechanisms which address the issue of inter-country personal data transfers (‘trans border data flows’ in Organization for Economic Cooperation and Development (OECD) terminology). A Data Privacy Subgroup was set up comprising Australia (the then chair), Canada, Chile, China, Chinese Taipei (Taiwan), Hong Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States. The United States and Canada have subsequently chaired the subgroup.

The proposals went through nine draft versions. After the first three versions were published on the internet, the chair declared that subsequent versions would not be available outside the subgroup and those with whom it consulted, until a ‘consultation draft’ was released. The early drafts had attracted some public criticisms. The subsequent drafts did become more widely distributed than the chair intended, but critiques external to the process were and remain very few in number.

Following are the Asia-Pacific Economic Cooperation (APEC) principles:

a) Preventing Harm: Its aim is to prevent any misuse of an individual’s personal information. Every privacy protection should be designed to prevent the wrongful collection and misuse of individuals’ personal information.

b) Notice: It ensures that individuals know what information is collected about them and for what purpose it is to be used. This principle binds the personal information controllers to provide a proper notice to an individual so that he or she could make an informed decision about interacting with the organization.

---

38) Ibid.
39) Supra note 35 at 95.
40) “APEC Privacy Framework,” available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/05_ejdbc_privacyframewk.ashx accessed on July 20, 2013, at 8:30 p.m. IST.
c) **Collection Limitation:** This Principle limits collection of information by reference to the purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant.

d) **Uses of Personal Information:** The Use Principle says that the personal information should only be used for the intended and other compatible or related purposes.

e) **Choice:** This principle makes it compulsory that the individuals should be provided with a choice in relation to collection, use, transfer and disclosure of their personal information. The notice of such choice should be clearly asked in words and displayed clearly and conspicuously either on the website or any other form.

f) **Integrity of Personal Information:** This Principle binds a personal information controller to maintain the accuracy and completeness of individuals’ personal information and keep it up to date. It is quite possible that a wrongful decision can be made out on the basis of inaccurate, incomplete or outdated information. Consequently, it would neither be in the interest of individuals nor organizations.

g) **Security Safeguards:** Its aim is to provide reasonable security safeguards to the individuals’ personal information.

h) **Access and Correction:** Every individual has a right to access and correct his personal information. However, such right is not an absolute one. This Principle says that there should be specific conditions for reasonable access which include conditions relating to time, fees, and the manner and form in which access would be provided.

i) **Accountability:** This principle makes personal information controller accountable for executing the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that
the recipient person or organization will protect the information consistently with these Principles.41

4.5 Right to Privacy in United States

In United States, the concept of ‘privacy’ can be understood by tracing it through the historical evolution of postal communications. The privacy of postal communications in colonial America was not up to the mark. It was the British Government who brought significant changes in the postal services in America. It also gave the formal recognition to the importance of postal privacy. During the reign of Queen Anne, the Parliament adopted the Post Office Act of 1710, which provided that no person shall presume wittingly, willingly, or knowingly, to open, detain, or delay, or cause, procure, permit, or suffer to be opened, detained, or delayed, any Letter or Letters, Packet, or Packets. The Act also prescribed a fine for the wrongdoers. In addition, each postal employee was required to take the Oath for the protection of privacy matters written in the letters. For every seizure of mail, the prior warrant was required. This shows how seriously British subjects valued the privacy of their correspondence.42

The seeming public indifference to the invasions of telegram privacy was due largely to the deference typically given to the government in time of war. There is a general consensus that when an armed conflict is occurring, the niceties of constitutional law are not necessarily observed. But equally important was the fact that at the time, the concept of privacy had not expanded to encompass much beyond one’s home and postal correspondence, and virtually no attempts had been made by the judiciary to rein in the search and seizure activities of federal agents. The Fourth Amendment, guaranteeing freedom from unreasonable searches and seizures, except upon the issuance of a warrant, lay largely dormant: in nearly a century of federal court decisions between 1787 and 1865, the amendment was directly cited just twice. But in the latter part of the nineteenth century, the attention paid to the Fourth Amendment, and to the practice of governmental search and seizure in general, grew rapidly.43

In the history of the right to privacy, the distinction between the telegraph and the telephone can be seen clearly by virtue of the fact that for the first seventy-five years or so of its existence, the telegraph did not generate a single significant court ruling on privacy. The telephone, however, thanks in part to its ubiquity and in part to the relative ease with which law

---

1. Ibid.
2. Frederick S. Lane, American Privacy, 6 (2009).
3. Id., at 33.
enforcement could eavesdrop on personal conversations, quickly sparked legal controversies that substantially shaped the development of the law of privacy.  

In theory, the invention of the telephone in the late nineteenth century should have been a positive development for the privacy of personal communications. The transmission of one’s voice directly to the ear of a listener meant that there was no writing involved that could go astray or be read en route by someone other than the intended recipient. And whereas sending a telegram necessarily required presenting the message to the telegraph operator, when using the phone there was no need to reveal the content of one’s conversation ahead of time to the phone company, and thus no need to trust that the conversation would remain secure in the company’s records. Even the casual eavesdropping that can occur in the street or in a shop was largely eliminated by the marvelous new invention.

But in reality, the telephone inflicted grave and permanent damage to the concept of personal privacy. Part of the reason was the end of a certain amount of psychological solitude: to a degree never matched by the silent letter or even the telegram delivered to the door, the telephone was a self-inflicted breach in the wall of the subscriber’s castle. Once a phone was installed, its demanding jangle could sound at any moment. As numerous commentators grumpily noted at the time, whatever its other merits, Bell’s telephone sadly reduced the peace and serenity previously enjoyed in one’s home.

But the most significant impact of the telephone on personal privacy was the launch, once and for all, of the era of electronic exhibitionism and voyeurism. The inherent characteristics of the new technology made it remarkably easy for nosy neighbors and aggressive law enforcement officers to listen in on virtually any telephone conversation. The growth of both casual and intentional eavesdropping that accompanied the invention of the phone permanently changed not only society but the law that governs it.

In the century and a half since its invention, photography has had a profound impact on personal privacy and continues to evolve in ways unimaginable to Daguerre (photography’s inventor). In particular, the recent development of digital photography is challenging and reshaping our understanding of personal privacy on a daily basis. It would be some years,

\[\text{Id. at 77.}\]
\[\text{Ibid.}\]
\[\text{Id., at 78.}\]
however, before the impact of photography on personal privacy would be fully felt in Daguerre’s time.48

The Fourth Amendment49 was enacted in 1791 in response to 18th Century English and Colonial experience with general warrants and writs of assistance. Although enacted in 1791, the Fourth Amendment did not play a major role in the law of criminal investigations in the period before the Prohibition Era of the 1920s. This is true for three reasons. First, the Fourth Amendment only applied to the federal government, while most crimes and investigations occurred at the state and local level. Second, the absence of trained federal criminal investigators meant that federal agents obtained and executed warrants relatively infrequently. Third, Congress did not create an automatic right to appeal a federal criminal conviction until 1889, meaning that most criminal cases ending in conviction were final when the defendant was sentenced. The combination of few investigations and few appeals meant that the courts had few opportunities to explain and interpret the Fourth Amendment. As a result, it remained unclear during most of the 19th Century whether the Fourth Amendment granted a broad right to privacy against invasive government investigations, or, much more modestly, it simply regulated the type and format of search warrants.50

As claimed, the American courts had already recognized a legally protected interest in personal privacy in different forms even before Samuel D. Warren and Louis D. Brandeis’ article entitled “The Right to Privacy” in 1890. Doctrines of trespass, eavesdropping, defamation, unreasonable search and seizure, sanctity of the mails, and confidentiality of census information were recognized as part of ‘privacy’ of the individual by State and Federal courts.51

Furthermore, Jed Rubenfeld52 claimed that Marbury v. Madison53 was a progenitor of the right to privacy decisions because it too belongs to the diverse series of cases in which the

---

48 Id., at 21.
49 The United States Constitution, Fourth Amendment provides: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
Supreme Court has reached out beyond the express language of the Constitution and struck down on constitutional grounds some piece of federal or state legislation.

The famous phrase, the right ‘to be let alone’ has also a long history. As far back as 1834, the United States Supreme Court mentioned in the case of Wheaton v. Peters54 that a defendant asks nothing- wants nothing, but to be let alone until it can be shown that he has violated the rights of another.55 The phrase, ‘the right to be let alone’, also appears in a Cooley’s text book, as corresponding to the duty ‘not to inflict an injury’, for example, by battery.56 This argument was expanded by Warren and Brandeis in their famous law review article. Subsequently, Brandeis used the phrase ‘the right to be let alone’ in his famous dissent in Olmstead v. U.S.57 the first wiretapping case heard by the United States Supreme Court. The ‘right to be let alone’ is the most terse definition of the right to privacy, although, through numerous United States Supreme Court decisions cited later in this article, this phrase has come to be associated with preventing invasions of the private sphere by the government.58

Again, the modern concept of the Right to privacy has been developed by the innovative potential of the courts. In United States of America, when the Constitution and Bill of Rights were ratified, neither statutes nor common law rules established a right of privacy as such. And certainly there was no constitutional provision which clearly provided a vehicle for its inclusion. The common law with regard to trespass, assault, slander and libel, and even nuisance (as applied to offensive noises and odors for example) could be said to have tangential reference to privacy, but this would offer a piecemeal approach rather than an argument based on a full-fledged right of privacy.59

Many thinkers also claim that the law of privacy in United States was originated with the publication of an article entitled “The Right to Privacy” in Harvard Law Review in the year 1890, authored by two Boston lawyers i.e. Samuel D. Warren and Louis D. Brandeis. It was

---

55 Id., at 634.
57 277 U.S. 438, 478 (1928).
58 Ronald B. Standler,“Privacy Law in the USA”, available at [http://www.rbs2.com/privacy.htm#anchor222222](http://www.rbs2.com/privacy.htm#anchor222222) accessed on July 1, 2012, at 8:00 p.m. IST.
59 M. Glenn Abernathy, Civil Liberties under the Constitution, 94 (1977).
stated that the authors invented a brand new tort i.e. the invasion of privacy. Dean Roscoe Pound, reportedly said that the article did nothing less than add a chapter to the law.60

Warren and Brandeis began by noting new technological developments that were posing a potential threat to privacy and focused on how the common law could develop to protect the interest then called ‘privacy’. The authors, however, did not spend much time setting forth a conceptual account of privacy.61 Warren and Brandeis defined privacy as the ‘right to be let alone,’62 a phrase adopted from Judge Thomas Cooley’s famous treatise on torts in 1880. Cooley’s right to be let alone was, in fact, a way of explaining that attempted physical touching was a tort injury; he was not defining a right to privacy. Warren and Brandeis’s use of the phrase was consistent with the purpose of their article: to demonstrate that many of the elements of a right to privacy existed within the common law.63

The authors declared that the underlying principle of privacy was ‘that of inviolate personality.’64 They noted that the value of privacy is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all.65 Warren and Brandeis observed that increasingly modern enterprise and invention have, through invasions upon his privacy, subjected [an individual] to mental pain and distress, far greater than could be inflicted by mere bodily injury.66 The authors noted that this type of harm was not typically protected by tort law. While the law of defamation protected injuries to reputations, privacy involved ‘injury to the feelings,’ a psychological form of pain that was difficult to translate into the tort law of their times, which focused more on tangible injuries.67

Nearly forty years later, when he was a justice on the Supreme Court, Brandeis wrote his famous dissent in Olmstead v. United States.68 The Court held that wiretapping was not a violation under the Fourth Amendment because it was not a physical trespass into the home.

60 Id., at 95.
63 Supra note 61 at 1100.
64 Supra note 62 at 205.
65 Id., at 200.
66 Id., at 196.
67 Id., at 197.
68 Supra note 57.
Brandeis fired off a dissent that was to become one of the most important documents for Fourth Amendment privacy law, stating that the Framers of the Constitution "conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." 69

Brandeis’s article and his dissent played a major role in the development of the law of privacy. In *Katz v. United States*, 70 the United States Supreme Court adopted Brandeis's dissenting view, and overruled its earlier judgment delivered in *Olmstead v. United States*. 71 In its Fourth Amendment jurisprudence, as well as its substantive due process protection of the right to privacy, the Court frequently has invoked Brandeis’s formulation of privacy as "the right to be let alone." 72

The formulation of privacy as the right to be let alone merely describes an attribute of privacy. Warren and Brandeis’s aim was not to provide a comprehensive conception of privacy but instead to explore the roots of a right to privacy in the common law and explain how such a right could develop. The article was certainly a profound beginning toward developing a conception of privacy. 73

In the years following the publication of the article, a law of privacy gradually developed by statute and by common law decision in state courts. But it was not until 1965 that the United States Supreme Court squarely held that the Constitution contained at least a limited right to privacy. 74

The United States’ courts have developed privacy rights on a constitutional basis. Various amendments of the American Constitution like First, Third, Fourth, Fifth, and Fourteenth Amendments containing provisions protecting privacy interests has laid the necessary foundation for the courts in this regard. These amendments mainly protect informational privacy. 75

The privacy regarding decisional privacy was protected mainly using the ninth amendment. Evolution of privacy as a constitutional right in America was through cases which

---

69 Id., at 478
70 389 U.S. 347 (1967).
71 Supra note 57.
72 Id., at 1101.
73 Id., at 1102.
74 Supra note 59 at 95.
fell in categories of sexuality, search and seizure, eavesdropping, and Data protection and press.\textsuperscript{76}

The great peculiarity of decisional privacy cases in America is their predominant focus on sexuality. Nothing in privacy cases has stressed that doctrine must gravitate around sexuality; nevertheless it has. The American courts first announced the right to privacy in a case involving a statute prohibiting use and distribution of contraceptive devices to married couples. In a later case the American court invalidated a law criminalizing inter-racial marriage on the ground that it violated right to privacy.\textsuperscript{77}

In \textit{Griswold v. Connecticut}\textsuperscript{78}, a majority of the court indicated that the Constitution creates “zones of privacy” which are beyond the scope of any legitimate search, and held invalid the Connecticut law barring the use of any drug or instrument for contraceptive purposes. Justice Douglas, for the majority said:

\begin{quote}
[W]ould we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.\textsuperscript{79}
\end{quote}

In \textit{Eisenstandt v. Baird}\textsuperscript{80}, the court observed that if the right to privacy means anything it is the right of individual, married or single to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.

In \textit{Roe v. Wade}\textsuperscript{81}, the court struck down a Texas statute which prohibited almost all abortions. The court’s decision was based on the assumption that the right to abortion was part of a right of personal privacy. The court observed:

\begin{quote}
This right of privacy whether it be founded in the 14\textsuperscript{th} amendment concept of personal liberty and restrictions upon state action, as we feel it is or as the district court determined, in the 9th amendment reservation of rights, is broad enough to compass a woman’s decision whether or not to terminate her pregnancy.\textsuperscript{82}
\end{quote}

\begin{thebibliography}{99}
\setlength{\itemsep}{1pt}
\bibitem{76} \textit{id.}, at 53.
\bibitem{77} \textit{ibid.}
\bibitem{78} 381 U.S. 47 (1965).
\bibitem{79} \textit{id.}, at 485.
\bibitem{80} 405 U.S. 438 (1972).
\bibitem{81} 410 U.S. 113 (1973).
\bibitem{82} \textit{id.}, at 115.
\end{thebibliography}

128
The private right to marry whom one chooses has been at the heart of due process judicial cases since the early 1960s. Laws that generally limit one’s choice in marriage or that tend to restrict the rights of a class of persons to marry will not be upheld unless the state can show a compelling interest in the restriction or in maintaining the classification. Loving v. Virginia represents an early Supreme Court case that established the fundamental constitutional right to marriage and the notion that laws restricting this right should be subject to the strictest of scrutiny under the Due Process and Equal Protection clauses of the Fourteenth Amendment of the United States Constitution. The Supreme Court unanimously decided Loving v. Virginia, and Chief Justice Earl Warren delivered the opinion.

The decision in Loving v. Virginia concerned the legality of anti-miscegenation statutes, which were laws that banned the mixing of different ethnicities, especially in marriage. The Supreme Court declared the Virginia statutes unconstitutional and thus ended all race-based legal restrictions on marriage in the United States. At the time Loving v. Virginia was decided, Virginia was one of 16 states that prohibited and punished marriages on the basis of racial classifications.

The constitutional right to privacy, however, is not an absolute right. It can be curtailed on the ground of compelling social interest or in the interest of basic competing right of other individuals.

In America, the fourth and fifth Amendments provide the necessary safeguards against arbitrary search. After a very long debate the United States Supreme Court adopted the wider approach and overruled the narrower approach of its own Augustus fraternity in Katz v. United States. Stewart J. wrote that although a closely divided court supposed in Olmstead that surveillance without any trespass and without seizure of any material object fell outside the ambit of the constitution, we have since departed from the narrow view on which that decision rested. Indeed we have expressly held that fourth amendment governs not only the seizure of

---

84 388 U.S. 1 (1967).
85 Ibid.
86 Ibid.
87 Ibid.
88 Supra note 83 at 330.
89 Supra note 75 at 55.
90 Supra note 70.
tangible items but extends as well to the recording of oral statements, overheard without any technical trespass.\textsuperscript{91}

More interestingly, the United States Supreme Court in the case of \textit{Stanley v. Georgia}\textsuperscript{92}, ruled that the First and Fourteenth Amendments of the United States Constitution prohibit the government from criminalizing the mere possession of obscene material if the material is held privately.\textsuperscript{93} The Supreme Court drew a clear distinction between this case and its previous line taken in earlier cases that allowed states to criminalize pornography that was either sold or distributed to the public. In this case, the Supreme Court focused on the much more limited reach of the obscene material, in that it was merely possessed in the privacy of the defendant’s home. The sanctity of privacy in one’s own home convinced the court to declare unconstitutional the Georgia criminal statute against obscenity at issue in the case.\textsuperscript{94}

All these cases involved traditional searches. The Court’s decisions directly addressing application of the Fourth Amendment to physical and transaction surveillance have been similarly restrained. That conclusion might seem to be contradicted by the most prominent recent Supreme Court case concerning surveillance, \textit{Kyllo v. United States}\textsuperscript{95}, decided in 2001. The Court prohibited the use of a thermal imager to detect heat differentials inside a home unless authorized by a warrant based on probable cause. But this judgment also indicated that if the domestic spying relies on technology that is in “general public use,” it may occur without any justification at all. This aspect of judgment potentially opens a huge hole in the holding. In other decisions, the Court has concluded that Fourth Amendment protection also disappears whenever the physical surveillance monitors activities outside the home, regardless of the type of technology used.\textsuperscript{96}

In United States, however, the passage of Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) broadened the existing law enforcement tools, particularly in the area of surveillance and internet. Prior to its enactment, investigators in terrorism and espionage cases were required to return to the court every time a suspect changed telephones or computers and

\begin{flushleft}
\textsuperscript{91} \textit{ld.} at 353.
\textsuperscript{92} 394 U.S. 557 (1969).
\textsuperscript{93} \textit{ld.} at 568.
\textsuperscript{95} 533 U.S. 27 (2001).
\textsuperscript{96} Christopher Slobogin, \textit{Privacy at Risk}, 16 (2007).
\end{flushleft}
obtain a fresh warrant. The Act allows ‘roving wiretap’ warrants from a secret court to intercept a suspect’s phone and Internet conversations, without identifying a specific phone or the suspect. In other words, when the target of a roving wiretap order enters another person’s home, law-enforcement agents can tap the homeowner’s telephone. According to the American Civil Liberties Union, the Federal Bureau of Investigation already has broad authority to monitor telephone and Internet communications. Current law already provides, for example, that wiretaps can be obtained for the crimes involved in terrorist attacks, including destruction of aircraft and aircraft piracy. Most of the changes to wiretapping authority contemplated in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) would apply not just to surveillance of people suspected of terrorist activity, but to investigation of other crimes as well. The FBI also has authority to intercept communications without probable cause of crime for ‘intelligence purposes under the Foreign Intelligence Surveillance Act (‘FISA’). The standards for obtaining a FISA wiretap are lower than those for obtaining a criminal wiretap.97

Pen registers and trap-and-trace devices electronically screen telephone or Internet communications. So, a pen register monitors all numbers dialled from a telephone line or all Internet communications are recorded. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) authorizes a federal judge or magistrate in one area to issue a pen register or a trap-and-trace order that does not specify the name of the Internet Service Provider (ISP) upon which it can be served. Indeed, it can be served on an ISP anywhere in the United States. The judge simply issues the order and law-enforcement agents fill in the locations at which the order can be served, thereby further curtailing the judicial function.98

4.5.1 Historical Tussle between Privacy and Media in United States

America was a rural nation during, and for many decades after, the colonial period. Villages, farms, and other living units were usually far apart. And within villages there was generally great similarity in nationality, background, habits, and taste, providing little stimulation to spy into another person’s beliefs, attitudes, or activities. The population of the nation was relatively small. Paradoxically, while considerable physical distance existed between villages

---

98 Id., at 75.
and residences, little privacy was possible within most homes and in most places of public accommodation and work.  

The press of the late eighteenth and early nineteenth centuries was also significantly different than it would be in 1890. Politically oriented, the newspapers of the day were more interested in opinion and comment than in news. And the comment was directed at nothing as mundane as the private life of the average man; only political or public men were important and newsworthy. The press of this era directed to an elite group—those who could read. Its content, therefore, reflected a higher standard than if it had been intended for a mass audience. In addition, the newspaper of this era was small both in size and in number.  

After civil war, which also destroyed the agrarian society, the industrial age was arriving. Beginning in the middle of the nineteenth century, the entire political, social, economic and cultural structure of the United States underwent a marked change. By 1890 the transformation had nearly been completed, and there existed a nation of urban dwellers who not only desired more privacy but probably needed it as well. The industrial revolution brought more rural inhabitants to urban areas to find work. The development of water systems, indoor plumbing, mass transit, electricity, the telephone, and other modern convenience made urban life more attractive. It led to the growth of American city. To fill up the vacancies of unskilled workers, the America’s population was increased by immigrants.  

With the increase in America’s population, the ideals of rugged individualism and self-reliance began to fade in the great urban sprawls. Dependence on others for food, drink, housing, clothing, medical care, police and fire protection, and many other services was a part of city life. While these services were frequently less than adequate, the urban dweller was compelled to interact with the society in order to survive. Add to this the close proximity in which families were forced to live in the overpopulated cities, and it should be apparent that physical privacy was difficult to attain.  

But in the urban environment the another kind of privacy, i.e. feeling of indifference towards friends and neighbours, was increased especially in the upper sections of the working class, the middle class and the elites. And such a feeling of indifference became one of the 

---

97 Don R. Pember, Privacy and the Press, 5 (1972).
98 Ibid.
100 Id., at 7
101 Id., at 7
102 Id., at 8
essential factors in the growth of privacy in the last half of the nineteenth century. In aggregate, the growth of urban America did play a role in the conceptualization of privacy as a legal entity.\footnote{Id., at 9}

The growth of the American press in the one hundred years after 1790 paralleled the development of the nation. The newspaper press experienced a small revolution in 1830s when the development of the penny press increased circulation and placed a greater emphasis on content interesting to the common man. More people could buy and read newspapers that cost only penny, and a kind of popular journalism emerged which featured more sensational, colorful, and, to the average reader, interesting news. The education was also being spread through compulsory education laws, and consequently it increased the number of readers. In result, the circulation of the newspaper was increased.\footnote{Id., at 10}

The growth of the press resulted into more business. Advertisements for department stores, patent medicines, laundry, soaps, baking powder, electricity or gas, etc. became the major source of revenue for the newspapers. Further, with the increase in the innovations like stereotyping, new photographic engraving processes, etc., the newspapers became able to package their news more attractively and get it to readers faster and cheaper than ever before. The people in the growing urban areas, bonded together in cultural and economic units, turned to the daily press for the story of their urban life and common interests. The newspapers started making salacious and lusty stories so that it would appeal the readers.\footnote{Id., at 12}

The new popular press in America while attracting a large following of avid readers also generated a number of critics. Intellectuals of the era scorned the sensationalism and poor taste of many of the big daily newspapers. And for the first time there was widespread criticism that the methods and techniques of the newspaper press were being used to invade the individual’s privacy. In 1890, the two Boston lawyers named as Samuel Warren and Louis D. Brandeis wrote an article regarding ‘Right to Privacy’ which was published in Harvard Law Review. There has been much speculation about why the article was written by them. Because the article exhibits the authors’ great dissatisfaction with the popular newspaper press of the day, this is often assumed to be the reason for the article.\footnote{Id., at 23}
Warren and Brandeis searched for the principle needed for protection against invasion of privacy. They found such a principle in the doctrine of common law copyright, which invests in an author or artist the executive right to make copies of his work for a limited period of time; it is automatic and lasts indefinitely, as long as no publication occurs.  

In addition to the law of literary property, Warren and Brandeis used a series of British and American cases involving breach of contract as a support for their proposal.  

However, Neil M. Richards and Daniel J. Solove argued that Warren and Brandeis did not invent the right to privacy from a negligible body of precedent but instead charted a new path for American privacy law. By 1890, a robust body of confidentiality law protecting private information from disclosure existed throughout the Anglo-American common law.  

Throughout the twentieth century, American privacy law began to embrace Warren and Brandeis’s right to privacy. In contrast, in England, the Warren and Brandeis article had a chilly reception and was rejected. Instead of creating a law of privacy, England developed a law of confidentiality, which was explicitly distinguished from privacy. Ironically, both the American law of privacy and the English law of confidentiality emerged from the same source—the Prince Albert v. Strange case.  

The American law of privacy evolved faster than in England. The growth of the British law on the subject seemed to climax in 1849 in Prince Albert v. Strange, because the participants included Queen Victoria and Prince Consort Albert. In this case, Queen and Prince made drawings and etchings for their own use only. The printer, who worked for the Queen and Prince, kept unauthorized copies of the drawings and etchings. Further, he gave them to William Strange, who planned to exhibit them. But the court stopped the exhibition by using injunction orders. It was held that it’s the violation of property right in the works which belonged to Victoria and Albert.  

Warren and Brandeis cited the above said case in their article and studied it in detail. They also relied on it for recognizing the idea of ‘privacy’. Generally, it is assumed that right to privacy was originated with the publication of their Article in 1890. Contrary to this viewpoint, it
is being held that even before their call for a new tort, some U.S. courts already recognized indirect legal protection for personal interests in privacy.  

In the twentieth century, privacy torts inspired by Warren and Brandeis’s article slowly developed and proliferated in the United States. Immediately after their article, the New York lower court recognized the right to privacy in the case of *Schuyler v. Curtis*. This case was related with the display of a statue of the great philanthropist (who was dead). The deceased philanthropist’s family members wanted the injunction order to stop the display on the grounds that it constituted an invasion of privacy. The lower court granted the injunction order in this regard. But later on the New York court of Appeals reversed the lower court’s decision on the ground that the right to privacy of the deceased had died with her.

In the case of *Roberson v. Rochester Folding Box Co.*, the court rejected the right to privacy and concluded that it has no place in the settled principles of jurisprudence. The court said that only legislature can enact this right.

But Judge John C. Gray gave the dissenting view and argued that right of privacy was already within the accepted principles of law.

The *Roberson* decision received strong criticism from both public as well as press. In response to the public criticism in 1903, the New York legislature enacted a privacy statute which allowing the people to sue for invasion of privacy where their name, portrait or picture was used without consent for advertising and trade purposes.

Later on, in 1905, the Georgia Supreme Court expressly disagreed with *Roberson* decision and recognized a common law cause of action for the unauthorized use of a man’s photograph in a life insurance advertisement. The court reasoned that no legislation was necessary because the right of privacy has its foundation in the instincts of nature.

Judicial recognition to the freedom of press and speech was also one of the important factors in the development of the law of privacy. In many cases, it was decided by the courts that publicity was absolutely essential to the welfare of the public. It was recognized that at certain times the rights of the individual must be secondary to the broad public right manifested in part

---

114 Supra note 109 at 146.

135
in the policy of the unfettered press. This kind of philosophy permeated the growth of the law of privacy.\textsuperscript{118}

In some cases, the lower courts of New York justified a privilege for news reporting on the rationale that subjects of coverage had effectively waived their interests in privacy by voluntarily thrusting themselves into the public arena. In others, courts relied on the public’s right to know to justify an exemption for news coverage of persons who found themselves caught up in newsworthy events, regardless of whether the subjects had sought attention.\textsuperscript{119} In many cases, where an individual became the public figure not by choice but by circumstance, the court refused to recognize the right to privacy of such an individual.\textsuperscript{120}

As 1930 closed, the right of privacy still had not found a secure place in the American jurisprudence. However, with the beginning of the next decade the law would grow at a more rapid pace. And with this development there were attempts to minimize the range of freedom enjoyed by the mass media in reporting news and current events. The protection established in the first thirty years of the century received a severe test.\textsuperscript{121}

In 1931, the California’s court, while stating that there was no such thing as common law of privacy, ruled that the plaintiff’s constitutional right of privacy had been violated. And this decision was the \textit{Melvin v. Reid}\textsuperscript{122}, in which a lady who had been a prostitute and also been convicted for a murder. On her acquittal, she did not want to remember her past life and tried to be rehabilitated. Of course she did it. She also married Melvin and started living respectful life with her husband and friends who were not aware about her past life. Later on the defendant made a motion picture called “The Red Kimono” which was based on her true story. The defendant also used her true name in the exhibition of the picture. The court took the help of California State Constitution which guaranteed some inalienable rights like right to pursue and obtain safety and happiness. The court concluded that such inalienable rights also include the right to live free from the unwarranted attack of others upon one’s reputation and social standing.

Meanwhile, the scope of legitimate public interest was also broadened up which definitely became the potent defence for the press. In \textit{Sidis v. F-R Publishing Corporation}\textsuperscript{123}, an

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{118} Supra note 99 at 77.
\item \textsuperscript{119} Supra note 113 at 1052.
\item \textsuperscript{120} Jones v. Herald Post Co. 230 Ky. 227 (1930). Cited in Supra note 99.
\item \textsuperscript{121} Supra note 99 at 94.
\item \textsuperscript{122} 112 Cal. App. 285 (1931). Cited in \textit{Ibid}.
\item \textsuperscript{123} 113 F. 2d 806 (2d Cir. 1940). Cited in \textit{Ibid}.
\end{itemize}
\end{footnotesize}
infant prodigy (plaintiff), who completed his graduation at the age of sixteen and also delivered a lecture on mathematics, attracted the attention of the public. But later on he started showing his negative attitude towards mathematics and public attention. He wanted to get rid of from the unnecessary publicity. Hence, he started living in solitude and engaged himself in some petty jobs. After so many years of his disappearance, the New Yorker magazine’s article revealed his all past as well as present activities. The plaintiff contended that such action really violated his right of privacy. But the court rejected his contention and held that the magazine’s article had news value. It was concluded by the court that the plaintiff was once a public figure and every fact about his disappearance was still a matter of public concern.

Therefore, gradually the test of newsworthiness was overriding the claim of privacy rights. The Court’s 1964 landmark decision in New York Times Co. v. Sullivan\(^{124}\) provided an even more important boost to journalists’ claims of constitutional privilege. The decision raised barriers to tort recovery against journalists for defamation by requiring plaintiffs who were public officials to show that any damaging falsehoods in news reports were made maliciously or with reckless disregard for the truth.\(^{125}\) The Court rationalized constitutional protection for some false statements on the ground that freedom of expression requires “breathing space” and that vigorous public debate must tolerate even occasional falsehoods so that participants will not be afraid to speak.\(^{126}\)

Further in one of the case the United States Supreme Court recognized the society which gives the primary value to freedom of speech and press.\(^{127}\) The Court held that the freedom of press assures the maintenance of political system and an open society.\(^{128}\)

However, the Courts started refusing to decide on ‘what is newsworthiness?’ or ‘what’s not’? So, the journalists’ and editors’ own conception of newsworthiness became the legal standard in privacy cases. The Second Restatement of Torts also adopted and recognized such kind of self-regulation system in defining the limitations of news reporting.

In past, the press played the significant role during three moments—the Civil Rights Movement, the Vietnam War, and Watergate. During this period, the courts also favoured

\(^{124}\) 376 U.S. 254 (1964).
\(^{125}\) Id. at 264, 280.
\(^{126}\) Id., at 272, 279–80.
\(^{128}\) Id., at 389.
freedom of press because the journalists had public regard. This was the time when investigative reporting was really doing something for public good. Whereas, today’s media is more concerned about their target ratings points (TRP) ratings and showing news regarding celebrities only, which doesn’t reflect any ‘public good’. The reality TV shows spreading the indecent values in the society. Hence, the media is losing the public support.

4.5.2 Informational Privacy Laws in United States

Although United States Constitution didn’t contain the term ‘privacy’, the U.S. Supreme Court derived ‘right to privacy’ from various Amendments, such as First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments to the United States Constitution. Right to information privacy was first recognized in the case of *Whalen v. Roe*. The Supreme Court upheld a New York law that required the state to maintain computerized records of prescriptions for certain drugs because the program did not pose “a sufficiently grievous threat”. In *Nixon v. Administrators of General Services*, the Court upheld the federal statute that required national archivists to examine written and recorded information accumulated by the president. The Court ruled that while the appellant has a legitimate expectation of privacy in his personal communications, but that right must be weighed against the important public interest in preservation of materials.

Indeed, two significant informational privacy laws, prevailing in United States, are the Privacy Act of 1974 and the Computer Matching and Privacy Act 1988. However, such laws do not regulate the collection and use of personal information held by private entities. These laws only cover the federal government databases. During 1970s, the excessive use of automated data systems to keep individuals’ private records really threatened peoples’ expectations of privacy. In response to such apprehension, in 1973, the Advisory Committee on Automated Personal Data Systems recommended a code of fair information practices, which is based on five principles:

1. Existence of personal data record-keeping systems should not be secret.

---

129 *Supra* note 113 at 1068.
131 *Id.*, at 600.
2. A person should have an alternative to find out what information about him is in a record and how it is used.
3. The person’s consent must be required, when the information is being used for unintended purpose.
4. The person should have an alternative to amend or correct records of personal information.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Therefore, The Privacy Act of 1974 establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.\[134\]

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act of 1974 by adding new provisions regulating the use of computer matching. Computer matching is the computerized comparison of information about an individual for the purpose of determining eligibility for Federal benefit programs, or for the purpose of recouping payments or delinquent debts under such programs. Generally, as per according to new provisions of the Act of 1974, the federal agencies now have to make an agreement with other agencies participating in computer matching. Such agreement must describe the details, purpose, and procedure for matching records. Thereafter, the agreement will be reviewed by a Data Integrity Board. The agencies also notify individuals and provide them the opportunity to refute any adverse information before denying or terminating a benefit or loan. Further, the problem regarding privacy protections in

\[134\] http://www.justice.gov/opcl/privacyact1974.htm accessed on April 30, 2012, at 5:30 p.m. IST.
cable communications is being diagnosed by the Cable Communications Policy Act of 1984 (CCPA). Directly or indirectly, cable companies have the potential to record personally identifiable information. Such information may include name, address, electronic mail address, telephone number, Social Security number, bank account number, etc. The cable operators also record subscribers’ viewing habits, channels’ watch-list, etc. Such type of information can easily reveal one’s preferences, tastes, and choices and so on. Increasingly, sophisticated technologies have made cable companies more potent to collect personal information. Under Cable Communications Act, customer’s consent is required in case of disclosing personal information. However, cable companies can disclose customer’s personally identifiable information in case where it is necessary to render or conduct legitimate business activity. Thus, cable operators may disclose customers’ personal information to third parties such as marketing companies, collection agencies, and companies that specialize in warehousing personal information and creating personal profiles. Indeed, this “legitimate business activity” exception means that personal information can be disclosed to almost anyone. Moreover, because of the legitimate business activity provision, cable companies are permitted to combine customers’ personal information with personal information obtained from third parties to construct enhanced databases and customer profiles.\(^{135}\)

Under the Cable Communication Policy Act, cable companies must provide a written notice of privacy practices to each subscriber at the time of entering into a cable agreement and at least once a year thereafter. The cable companies must inform the customer about every detail of collection, processing, disclosure, usage, and limitations of personal information. Under the Act, the government can ask for such personal information, but only after showing clear evidence that the customer is reasonably suspected of engaging in criminal activity and that the information would be material evidence in the case. At the same time, the customer must be given the right to appear in court and contest any claims made in support of the court order. Furthermore, a cable customer can amend or correct errors in the personally identifiable information records. Personally identifiable information must be destroyed by the cable company

If the information is no longer necessary for the purpose for which it was collected, and if there are no pending requests or court orders for such information.  

Similarly, the Video Privacy Protection Act of 1988 prohibits videotape service providers from knowingly disclosing information regarding a consumer’s rental or purchase of “prerecorded videocassette tapes or similar audiovisual materials.”

The Stored Communications Act (SCA) (18 U.S.C. 2701-2711) governs law enforcement’s access to stored, or temporarily stored, wire and electronic communications. It was enacted as Title II of the Electronic Communications Privacy Act 1986. The Stored Communications Act includes any backup copies of files in temporary electronic storage. Accordingly, it governs access to the subscriber records of various communications service providers, including Internet service providers (ISPs). If a communication is being transmitted from its origin to a destination, then the Wiretap Act applies. If it is stored in the computer of a provider of an electronic communication service (ECS) or a remote computing service (RCS), then the Stored Communications Act governs.

In 1998, the Federal Trade Commission (FTC) reported widespread collection and use of personally identifiable information of children without their parents’ knowledge or consent. In response, Congress passed the Children’s Online Privacy Protection Act, 1998. The Children’s Online Privacy Protection Act (‘COPPA’) specifically protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users. The Act took effect in April 2000. The Act was passed in response to a growing awareness of Internet marketing techniques that targeted children and collected their personal information from websites without any parental notification. The Act applies to commercial websites and online services that are directed at children.

As far as health information privacy is concerned, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed. The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected

136 Ibid.
138 http://epic.org/privacy/kids/ accessed on May 1, 2012, at 10:15 a.m. IST.
health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.\(^{139}\)

The Right to Financial Privacy Act of 1978 protects the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records. The Act was essentially a reaction to the United States Supreme Court's ruling in *United States v. Miller*,\(^{140}\) where the Court found that bank customers had no legal right to privacy in financial information held by financial institutions. Generally, the Act requires that federal government agencies provide individuals with a notice and an opportunity to object before a bank or other specified institution can disclose personal financial information to a federal government agency, often for law enforcement purposes.\(^{141}\) Similarly, Fair Credit Reporting Act 1970 protects the consumers' personal information holding by credit bureaus. Furthermore, Bank Secrecy Act 1970, Financial Services Modernization Act of 1999, etc. are those laws which protect personal information records being kept in private sectors. Besides, there are safe harbor principles for those companies who wish to do business with European Union member states. Such principles are self regulatory in nature. These were developed on lines of European Union Directive.\(^{142}\)

The researcher noticed that in United States, certain government groups, such as Federal Trade Commission, Internet Crime Complaint Center and National White Collar Crime Center, are effectively protecting individuals' informational privacy. In addition, privacy advocacy organizations like Electronic Privacy Information Center (EPIC), Privacy International (PI), and the Electronic Frontier Foundation, which are non-governmental groups are also potential advocates of privacy. It is submitted that Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) has enhanced the powers of law enforcement agencies to access personal records held by libraries, health insurance companies, bookstores, schools, businesses, and civil or nonprofit organizations. With the passage of this Act, Fourth Amendment of United States' Constitution has also been diluted. Thus, it has become easier for law enforcement agencies to obtain personal records from financial institutions, telephone companies, and Internet service providers.\(^{143}\)

\(^{139}\) \url{http://www.hhs.gov/ocr/privacy} accessed on May 1, 2012, at 10:30 a.m. IST.

\(^{140}\) 425 U.S. 435 (1976).

\(^{141}\) \url{http://epic.org/privacv/rfpu/} accessed on May 1, 2012, at 10:35 a.m. IST.

\(^{142}\) Ibid

\(^{143}\) Ibid
4.6 Privacy in the United Kingdom

According to the Master of the Rolls, Lord Neuberger, in a speech given at Eton, there is no general right of privacy in United Kingdom. He points out that this was confirmed by the Court of Appeal in the Kaye v. Robertson, and reaffirmed by the House of Lords in Wainwright v. Home Office. In Kaye v. Robertson, the British actor Gordon Kaye met an accident and suffered serious head injuries. He was not in a fit state of mind to give any informed consent to the interview. A photographer and a journalist visited Kaye without obtaining any permission from the hospital staff. They proceeded to interview and take photographs of him in his hospital bed. It was accepted by the Court of Appeal that Kaye had been in no fit state to give any informed consent to the interview, but there had been no unlawful entry into the hospital and no physical damage done to Kaye. However, the court adopted another way and granted an injunction in malicious falsehood- a cause of action that had not been raised by the claimants and which requires proof of falsity, malice, and financial loss- to prevent the paper from alleging in its article that he had consented to the interview. But Lord Bingham expressed the dissatisfaction on the lack of an English Privacy law as follows:

The defendants’ conduct towards the plaintiff here was a monstrous invasion of privacy. If ever a person has a right to be let alone by strangers with no public interest to pursue, it must surely be when he lies in hospital recovering from brain surgery. It is this invasion of privacy which underlies the plaintiff’s case. Yet it alone, however gross, does not entitle him to relief in English law.

There is another interesting case of Wainwright v. Home Office, whose facts were taken place before the Human Rights Act came into force in October 2000. In this case, a woman and her psychological ill son were strip-searched by prison officers. The searches were conducted against the prison’s rules and guidelines. The Lord Chief Justice of the Court of Appeal said that the Human Rights Act could not be relied on to change substantive law by introducing a retrospective right to privacy which did not exist at common law. Thereafter, the matter went to the House of Lords, where the Lords were invited to declare that the gradual

---

146 Supra note 144.
147 Bernstein v. Skyviews Ltd, (1978) QB 479 at 489G.
148 Supra note 145.
absorption of Article 8 into English law had been completed to such a degree by 1997 that the law lords would have protected Article 8 rights by then. However, the House of Lords rejected the invitation. Lord Hoffmann concluded in October 2003 that the woman and her son had no right to sue for invasion of privacy. Lord Hoffmann rejected the invitation to declare that since 1950 there has been a previously unknown tort of invasion of privacy.\textsuperscript{149}

While referring the House of Lords’ decision of \textit{Wainwright v. Home Office},\textsuperscript{150} Lord Neuberger said:\textsuperscript{151}

In that case the Lords were invited to find that the Human Rights Act 1998 had introduced a right to privacy into English law. The invitation was flatly rejected. The Lords would not declare that there was a consequence of the 1998 Act ‘a previously unknown tort of invasion of privacy’ in English law. In doing so they were acting as Lord Hoffman had it, consistently with the jurisprudence emanating from Strasbourg. How? Because as he put it, Strasbourg has held that the article 8 right to respect for privacy does not require a State to provide a high level, general, privacy law.

However, although there is no general right to privacy in the United Kingdom, the right to respect for privacy has led the courts to develop a number of rights to allow for legal enforcement of the right to respect for privacy, particularly breach of confidence which had been developed so that there no longer needs to be confidential relationship between the parties in the dispute leading to a tort of misuse of private information.\textsuperscript{152}

But things began to change with the implementation of the Human Rights Act 1998 (the HRA) incorporating into United Kingdom law the European Convention of Human Rights (the Convention), and the Article 8 right protecting privacy. With the global spread of information, it is also impossible to ignore the rulings of the European Court of Human Rights (ECHR), whose long fingers probe the domestic laws of every member country.\textsuperscript{153} Lord Nicholls said in

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{149} Id., at para 35.
\item \textsuperscript{150} Supra note 145.
\item \textsuperscript{151} Quoted in Chris Frost, \textit{Journalism Ethics and Regulation}, 99-100 (2011).
\item \textsuperscript{152} Chris Frost, \textit{Journalism Ethics and Regulation}, 100 (2011).
\end{itemize}
\end{footnotesize}
Campbell v. MGN,\textsuperscript{154} that the protection of various aspects of privacy is a fast developing area of the law in the common law jurisdictions. Indeed, in Douglas v. Hello! Ltd\textsuperscript{155} and Von Hannover v. Germany,\textsuperscript{156} it was declared that the courts have a duty to recognise and protect privacy rights.

Historically, in 1361, the Justices of the Peace Act in England provided for the arrest of peeping toms and eavesdroppers. Moreover, the common law principles protect a person’s private home. In Semayne’s\textsuperscript{157} case, it was said that the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose. In 1765, British Lord Camden, striking down a warrant to enter a house and seize papers wrote, “We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have.” Parliamentarian William Pitt wrote, “The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.”\textsuperscript{158}

The earliest English cases which granted relief for what would be called today a violation of the right of privacy strove mightily to rest their decisions on some historically respectable ground, such as implied contract, breach of trust or confidential relationship defamation of character or the violation of a property right.\textsuperscript{159}

It has been observed that the English courts asserted ‘privacy interests’ in three sets of ‘boundaries’ during the period from nineteenth century to 1980s. The first boundary is being called as physical boundary. Such physical boundary was used to protect one’s ‘private property,’ especially one’s dwelling house. Such boundaries create a three-dimensional ‘private space’ given legal protection against some (but certainly not all) unwanted intrusions of outsiders. They are also barriers to the penetration of legal analysis: the interest in the privacy of private property may be asserted to prevent intruders from seeing something, from hearing something, or just from rendering the occupants uncomfortable. To the extent that the law

\textsuperscript{154} (2004) UKHL 22.
\textsuperscript{155} (2003) 3 All E.R. 996.
\textsuperscript{156} 2004-VI Eur. Ct. 41.
\textsuperscript{158} www.privacyinternational.org accessed on November 6, 2010
respects these boundaries, the motive of concealment behind them is irrelevant. The amount of available legal protection will vary according to other factors, including the means of intrusion and the official or unofficial status of the intruder.  

The second set of boundaries, those marking out confidential communications, are less tangible than the physical boundaries of private property. Property in the contents of a literary work is a concept familiar to the common law, one capable of extension to the contents of a diary and a personal letter. A property basis for the protection of telephone conversations or face-to-face communication is more difficult to imagine. Grounded on a variety of legal doctrines, protections of confidentiality are sometimes dependent on the means of communications employed, sometimes on the relationship between the speakers. Like the protections of physical property, they are never treated as absolute barriers to disclosure. Thirdly, and least tangible of all, are the boundaries around personal information concerning private individuals, information that may be inchoate and unexpressed until reduced to gossip or dossier by the invasion of privacy.

Again, the boundaries are permeable and the protections they afford are variously grounded. Information about which a person could not be compelled to testify may be given up by that person for statistical, financial, or medical purposes on the understanding, enforceable by law, that the information shall not be used for any other purpose. There is also some legal recourse if personal information is published broadly to the subject's embarrassment or annoyance, through extensions of the law of defamation and that of breach of confidence. As in the era of Warren and Brandeis, this set of boundaries is the focus of the greatest concern and the greatest uncertainty.

It should be obvious that the three sets of boundaries just described can sometimes offer overlapping protection to a unitary interest in privacy. Personal information may be communicated confidentially within the private property of the subject. If, for example, a husband communicates some matter of great delicacy concerning himself to his wife in the bedroom of their home, the law may afford protection from physical or mechanical eavesdroppers on the basis of private property, while it may allow the wife to refuse to testify to

---

161 Ibid.
162 Ibid.
(and permit the husband to enjoin the wife from publishing) the confidential communication, and
moreover it may shield the husband from forced disclosure himself on the basis of personal
information. In evolving all of these legal protections, however, English courts have treated the
categories as distinct ones, and have applied the language of privacy to all three.\textsuperscript{163}

4.6.1 Doctrine of Breach of Confidence

Prior to the enactment of the Human Rights Act 1998 (‘the HRA’), the ‘right’ could only
be established by combining several different common law and European law strands.\textsuperscript{164}

The concept of confidentiality as a value essential to a variety of personal relationships
can be traced back to antiquity. For example, in the physician-patient context, the Hippocratic
Oath (400 B.C) recognizes the confidential relationship between them. Confidentiality (or
“confidence” to use its earlier terminology) is a concept with ancient origins in the Anglo-
American common law as well.\textsuperscript{165}

An individual’s personal information is being protected from any misuse under the
common law and statute. Furthermore, the ‘confidential’ information also gets the protection
under the common law of breach of confidence. The law of breach of confidence is based on the
case of \textit{Prince Albert v. Strange}.\textsuperscript{166} an 1848 case in which Prince Albert obtained an injunction
to prevent the exhibition of etchings by himself and Queen Victoria in circumstances where the
defendant had obtained copies of the etchings without consent. Although the law was
subsequently developed to protect secret processes, inventions and trade secrets, its boundaries
have been constantly pushed back, and in recent years it has been used more and more to prevent
the publication of ‘confidential’ information in the media. An action for breach of confidence
and an injunction is the most appropriate method for an individual to prevent the publication of
confidential information about him.\textsuperscript{167}

The Breach of confidence was recognized as a separate tort remedy in the case of
\textit{Saltman Engineering Co. v. Campbell Engineering Co.}.\textsuperscript{168} Further in the case of \textit{Argyll v. Argyll}\textsuperscript{169} the court strongly supported \textit{Saltman’s} decision and held that remedy of breach of

\textsuperscript{163} Id., at 334.
\textsuperscript{165} Supra note 109 at 133.
\textsuperscript{166} Supra note 111.
\textsuperscript{168} (1963) 3 All E.R. 413 (1948).
\textsuperscript{169} (1967) Ch. 302.
confidence is also available in personal relationships and not just confine to commercial relations.

In one of more significant cases, *Coco v. A.N. Clark (Eng’rs) Ltd.*\(^{170}\), the court formulated three elements to identify the breach of confidence tort. The first was that the information should be confidential in nature and the second was that it should have been imparted in circumstances importing a duty of confidence. And third, there must be an unauthorized use of that information to the detriment of the party communicating it.\(^{171}\)

The law of confidence also covers government secrets, such as diaries of a Cabinet minister.\(^{172}\) It means that the government does rely on the law of confidence against the publication of government secrets.\(^{173}\)

The law of confidence was redefined by Sir John Donaldson in 1990. Since then the courts in a number of important cases confirmed that the right to the confidentiality of information is being recognized and maintained in United Kingdom. Sir John Donaldson’s view was that since the right to have confidentiality maintained is an equitable right, it will (in legal theory and practical effect if the aid of the court is invoked) bind the conscience of third parties, unless they are bona fide purchasers for value without notice. However, he qualifies this by saying that the right will be lost or, at all events, the courts will not uphold and enforce it, if there is just cause or excuse for communicating the information, and the right will also be lost if the information, which is subject to a right of confidentiality, is published to the world by or with the consent of the confider, but it will not unnecessarily be lost if such publication is by the consent or with the consent of the confidant.\(^{174}\)

In *Barrymore v. News Group Newspaper*,\(^{175}\) Michael Barrymore obtained an injunction in confidence against the *Sun* after a man called Paul Wincott told the newspaper about his homosexual relationship with the television personality. In one of another case Justice Rose restrained the publication of a story obtained from health service workers which named two doctors with Acquired Immuno Deficiency Syndrome (AIDS). He said that the public interest in preserving the confidentiality of hospital records outweighed the freedom of the press to publish...
such information. In a later case, the courts upheld an order restraining the Mail on Sunday from publishing the memoirs of a nanny who had looked after the Blair’s children on the grounds that a duty of confidence was owed in these circumstances.\textsuperscript{176}

Since 1961, many bills were presented before the Parliament, and aimed at introducing a statutory tort of privacy. All have been unsuccessful because of insurmountable problems in connection with establishing adequate definitions of the civil offence of privacy and acceptable defences. During the same period, there have also been various Government committees and Royal Commissions that have considered the same question, the most recent of which was the Government Committee on Privacy and Related Matters chaired by David Calcutt QC, which reported in 1990. All recommended against the introduction of a statutory law of privacy on the basis of an unworkable definition of the tort and the undesirability of such a law.\textsuperscript{177}

By the late 1990s, the English law of confidence had a very broad scope that was gradually expanding. Courts had stretched the idea of an obligation of confidence quite far, interpreting it to include cases where there was not even any communication between the plaintiff and the recipient of the information, such as secret photography or wiretapping.\textsuperscript{178}

4.6.2 The Human Rights Act, 1998

In 1997 the New Labour government entered government with a landslide majority. Among its manifesto pledges was a commitment to incorporating the European Convention on Human Rights (ECHR) into United Kingdom law and the introduction of freedom of information legislation. In 1998, Parliament passed the landmark Human Rights Act (HRA), which came into effect in October 2000. The Human Rights Act of 1998 tied the United Kingdom to the European Convention on Human Rights (ECHR) and guaranteed human rights protection within United Kingdom law. Given that the United Kingdom does not have a written constitution which guarantees freedom of speech or the right to privacy, the Human Rights Act enables the right to privacy (European Convention on Human Rights (ECHR) Article 8) and the right to freedom of expression (European Convention on Human Rights (ECHR) Article 10) to be enshrined into United Kingdom law.\textsuperscript{179}

\textsuperscript{176} Supra note 152.
\textsuperscript{177} Supra note 164 at 114.
\textsuperscript{178} Supra note 109 at 166.
\textsuperscript{179} John Steel, \textit{Journalism and Free Speech}, 102 (2012).
The Human Rights Act of 1998 effectively incorporated a Bill of Rights into English law by requiring that English courts protect the rights guaranteed by the Council of Europe’s European Convention on Human Rights (ECHR). Two provisions of the European Convention on Human Rights (ECHR) have proven significant for English confidentiality law i.e. Article 8 and Article 10 which provides that everyone has the right to respect for his private and family life, his home and correspondence and everyone has the right to freedom of expression. The passage of the Human Rights Act has spawned a flurry of cases involving celebrities suing the media. Although the law remains in a state of flux, English courts responded to Article 8 not by endorsing a new action for privacy, but by further stretching the law of confidence. English law responded to Article 10 by holding that freedom of speech was a factor to be considered in the public interest exception to the tort.\textsuperscript{180}

In \textit{Douglas v. Hello! Ltd.},\textsuperscript{181} where the film stars Michael Douglas and Catherine Zeta-Jones sought an injunction order against the unauthorized publication of their wedding photographs, the court granted the relief on the basis of law of confidence only. In the opinion of the court, all three of the \textit{Coco} factors were satisfied—there was a quality of confidence because the information about the wedding was inaccessible, there was an obligation of confidence because the guests knew or should have known of the wishes of the bridal couple not to have photos taken, and there was detriment because the couple suffered both emotional and financial distress from the publication of the photographs.\textsuperscript{182}

The most important recent decision is that of the House of Lords in \textit{Campbell v. MGN Ltd.},\textsuperscript{183} Naomi Campbell brought proceedings when the Daily Mirror had published a number of articles revealing that she was receiving treatment at Narcotics Anonymous (NA) for drug addiction; they disclosed details of the treatment and were accompanied by pictures of the supermodel leaving a meeting of Narcotics Anonymous (NA). By a bare majority, the House of Lords upheld the claim that the publications infringed her privacy, but both Lord Hope and Baroness Hale, in the leading speeches for the majority, emphasized that the privacy interest was protected by an action for breach of confidence. In short, the courts in England are reluctant to recognize a general right to privacy, but are willing to protect privacy interests through well-
established causes of action, notably for breach of confidence, but also in appropriate circumstances by proceedings for trespass, nuisance and libel.184

The expansion of the doctrine of breach of confidence under the Human Rights Act began with the decision of Douglas v. Hello! Ltd.185 Section 6 of the Human Rights Act requires English courts to give effect to the rights in the Convention when developing the common law. There is no need to show a pre-existing relationship of confidence where private information is involved and the courts have recognised that the publication of private material represents a detriment in itself. The Human Rights Act has horizontal effect in disputes between private individuals meaning that the Human Rights Act is just as applicable as if one party had been a public body. Breach of confidence now extends to private information (regardless of whether it is confidential) so as to give effect to Article 8 of the European Convention on Human Rights.

Before this breach of confidence afforded ‘umbrella protection’ to both personal and non-personal information.186

As already mentioned, the House of Lords ruled in October 2003 that there is no general common law tort for invasion of privacy and that the European Convention on Human Rights does not require the United Kingdom to adopt the provisions of the convention.187 However, the House of Lords ruled in May 2004 that a tabloid newspaper violated model Naomi Campbell’s privacy under Article 8 by publishing that she was undergoing drug treatment and printing pictures of her leaving the treatment center.188

In Von Hannover v. Germany,189 the court dealt with a matter where paparazzi took pictures of Princess Caroline of Monaco, the eldest daughter of Prince Rainier III of Monaco. The subject matter of photographs was completely of private nature. The court held that the photographs did not refer to any public function but merely to Princess’s private life. Although the photographs were captured in the public place, they did not contribute any debate of general interest. The pictures were published only to satisfy the prurient tastes of few readers, and had no concern with the debate of general interest.

---

185 Supra note 155.
186 “Privacy in English law”, available at http://en.wikipedia.org/wiki/Privacy_in_English_law accessed on July 2, 2012, at 7:00 a.m IST.
187 Supra note 145.
188 Supra note 154.
189 Supra note 156.
Therefore, it will not be incorrect to say that the decision of the European Courts of Human Rights in *Von Hannover case* is much wider in scope than the House of Lords’ *Campbell case*. In *Campbell case*, Baroness Hale considered that a celebrity out and about buying a pint of milk in public at her local shop would be fair game. Such observation is being called as “the Milk Bottle Test”. But this would be unacceptable according to the principles of the European Convention on Human Rights (ECHR) decision in *von Hannover*. Although the press might consider itself after *Campbell* to be free to publish photographs of Naomi Campbell buying a pint of milk, after *von Hannover* they would not be free to do the same regarding the princess.190

### 4.6.3 Data Privacy in the United Kingdom

In the United Kingdom, the government set up the Younger Committee in the year of 1972. The purpose was to consider whether law was sufficient to tackle intrusions into privacy by private persons and organizations. Therefore, in that sense, Younger Committee was restricted to considering the private sector, plus the British Broadcasting Corporation (BBC) and United Kingdom universities. At that time, there was no specific law regarding right to privacy in England. Laws relating to trespass, nuisance, defamation and breach of confidence were being used to solve privacy issues. The Committee supported the remedy available in breach of confidence. This tort afforded a means of protection for all specific and reasonably implied confidences, except where the disclosure of the information given in confidence is shown to be in the public interest. The Committee recommended the law relating to breach of confidence should be promoted and clarified.191

The use of computing technology was taken seriously by Younger, with an entire section of the report devoted to the collection and handling of personal information and its possible misuse in the private sector. The Committee recommended 10 guiding principles for the use of computers that manipulated personal data. The principles, known as the Younger Principles, were become guidance for the Data Protection Act of 1984. Principles were about192:

- Purpose of data should be specified
- Authorized access to data

---


192 Id., at 242.
• Minimum holdings of data
• No personal identification in statistical surveys
• Subject should have access to data
• Security of data
• Security procedures for personal data
• Retention of data for limited period
• Accurate and up to date data
• Any value judgments should be coded

At that time, it was very clear that the United Kingdom had no legal control or regulation over automatic data processing. Against this backdrop, the government constituted a committee chaired by Sir Norman Lindop in 1976. The committee submitted its report, known as Lindop Report, in 1978. It was recommended that the scope of the legislation should extend to all automatic handling of personal data in the United Kingdom by any user, in both the public and private sectors. The report also recommended the creation of a Data Protection Authority and, proposed that the development and adoption of Codes of Practice for different sectors.

Meanwhile in 1980, Organization for Economic Cooperation and Development (OECD) adopted guidelines on the Protection of Privacy and Trans-border flows of Personal Data and in 1981 the Council of Europe Data Protection Convention. In response to this, Data Protection Act 1984 was passed. Like the convention, the Act of 1984 was only applied to regulate automatic processing of personal data and not manual processing of personal data. Finally, in order to update law, the Data Protection Act 1998 was passed on the lines of European Union Data Protection Directive 95/46/EC, and extended data protection law to some forms of manual processing and made other sweeping changes to data protection law.

4.6.4 The Data Protection Act, 1998

The British Parliament approved the Data Protection Act in July 1998 to implement the European Union Data Protection Directive. The legislation, which came into force on March 1, 2000, applies to records held by government agencies and private entities. It creates eight data protection principles based on the Directive to be followed. These provide for limitations on the

---

193 Id., at 246.
194 Id., at 247.
use of personal information, access to, and correction of, records, adequate security, and requires that entities that maintain records register with the Information Commissioner. The Office of the Information Commissioner is an independent agency that maintains the register and enforces the Data Protection and Freedom of Information Acts. The Commissioner is also responsible for enforcing the Privacy and Electronic Communication Regulations. Under the Enterprise Act 2002, the Commissioner can now apply for an enforcement order to a court for breach of the regulations. The Information Tribunal (formerly the Data Protection Tribunal) can hear appeals of decisions and notices. Interception of communications is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA). Part I authorizes the Home Secretary to issue warrants for the interception of communications and requires Communications Service Providers to provide a “reasonable interception capability” in their networks. The Home, Northern Ireland or Foreign Secretaries of State and the Scottish First Minister normally authorize telephone taps for national security purposes. It further allows any public authority designated by the Home Secretary to access “communications data” without a warrant. This data includes the source, destination and type of any communication, such as mobile phone location information and partial web browsing logs (but the full Universal Resource Locator (URL) is considered content subject to a warrant). Part III allows senior members of the civilian and military police, customs, and members of the judiciary to demand that users hand over the plaintext of encrypted material, or in certain circumstances decryption keys themselves. This has not been implemented yet, but the government held a consultation in 2006 on bringing it into force. Part II sets rules on other types of “human intelligence” powers that had not been previously regulated under United Kingdom law. The Privacy and Electronic Communications (EC Directive) Regulations 2003 came into force in December 2003. The regulations implement the European Union Directive on Privacy and Electronic Communications (2002/58/EC). They place new rules on cookies and require opt-in for most e-mail and short message service (SMS) spam.\footnote{Ibid.}

Furthermore, there has been a proliferation of Closed-circuit television (CCTV) cameras in hundreds of towns and cities in Britain. It is now estimated that there are over four million cameras in Britain, and the average citizen is recorded over 300 times each day. At present, the
cameras are being used by police, local authorities or private companies to prevent and detect crime. However, it has also been seen that the cameras seldom prevent or detect any crime.\(^{197}\)

The systems are increasingly being connected together with databases. In London, a system for "congestion charging" uses a sophisticated number plate recognition system to charge motorists who drive into central London during business hours. It was revealed that the system was organized in cooperation with the intelligence services that use it with facial recognition systems to monitor the drivers of the cars.\(^{198}\) The government announced in January 2005 that it was expanding its pilot program of Automatic Number Plate Recognition (ANPR) nationwide. Traffic cameras have also spread across the country. The Surveillance Commissioners in their annual report urged the Home Secretary to consider new legislation to authorize Automatic Number Plate Recognition (ANPR).\(^{199}\)

There has been growing criticism of the use of the cameras. The European Court of Human Rights ruled in January 2003 that a Council's release of Closed-circuit television (CCTV) footage of an attempted suicide for a campaign on Closed-circuit television (CCTV) violated the man's Article 8 right to privacy. Motorists across the United Kingdom have engaged in vandalism of traffic cameras and they are widely criticized for being used for fundraising rather than traffic safety.\(^{200}\) There is also a growing body of literature that the cameras are not nearly as effective as the proponents claim. A Home Office study released in 2005 found many problems with the systems. In all but one area studied, crime did not show a statistically significant decrease and even increased in a majority of areas for unknown reasons. Closed-circuit television (CCTV) also did not improve perceptions about safety significantly and did not change behaviors. In nearly half of the areas, support for Closed-circuit television (CCTV) and its perceived effectiveness declined once it was installed. On the design of the system, the study found that many systems were installed without clear objectives based on feelings that Closed-circuit television (CCTV) was 'a good thing,' a perceived need to 'catch up' if other jurisdictions had already installed them, and a pressure to bid for it based on the existence of funding more than actual need. Technical consultants were often not challenged on the installation of the

\(^{197}\) "Nowhere to Hide as Britain Tops CCTV League", \textit{Sunday Times}, April 18, 2004.


\(^{199}\) "PHR2006 - United Kingdom of Great Britain and Northern Ireland", available at \url{http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559479} accessed on November 6, 2010 at 12:00 p.m. IST.

systems and police were not consulted adequately. The Scottish Centre for Criminology found that the cameras did not reduce crime, nor improve public perception of crime problems. A study in June 2002 found that in many areas with Closed-circuit television (CCTV) crime increased and street lighting is a more effective deterrent.201

The United Kingdom is a member of the Council of Europe (CoE) and has signed and ratified the Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108) and the European Convention for the Protection of Human Rights and Fundamental Freedoms. The United Kingdom is a member of the Organization for Economic Cooperation and Development (OECD) and has adopted its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

4.6.5 Justice Leveson Inquiry Report, November 2012

In 2010, one of the oldest, reputed and United Kingdom based newspaper, News of the World, exposed the practice of spot-fixing in cricket. Consequently, Salman Butt and Mohammad Asif (famous players in Pakistan Cricket team) were found guilty by London Court. The News of the World has been winning the public support since 1843. It exposed many national or local celebrities as drug users, sex freaks or criminals. However, with the beginning of the year 2001, it was alleged that the newspaper’s under cover journalists’ were committing illegal phone-hacking. In 2005-06 the investigation reports concluded that the News of the World were hacking only politicians, celebrities and royal families’ phone numbers. But on 4th July 2011, the Guardian (another United Kingdom based newspaper) first revealed that an investigator working for the News of the World (NOTW), had hacked into the cell phone of the murdered teenager Milly Dowler.202 Actually, in 2002, Milly Dowler (who was 13 year old English girl), was abducted and subsequently murdered. The reporters of the News of the World hacked the voicemails of Milly Dowler and also deleted some potential evidences. Such deletion misled both parents as well as police investigations in finding the missing girl. Similarly it was also alleged that the newspaper in connivance with police also hacked the phones of family members of deceased British soldiers and victims of 7/7 London bombings. Therefore, this time the newspaper really attacked at the personal feelings of private individuals. Hence the

201 Supra note 199.
newspaper as well as its owner, Rupert Murdoch, both faced the public criticism. The newspaper also lost the money of its advertisers and finally the death of 168 years old newspaper took place.

Against the backdrop of phone-hacking scandal, The English Prime Minister, David Cameron, announced a two-part inquiry investigating the role of the press and police in the phone-hacking scandal, on 13 July 2011. Lord Justice Leveson was appointed as Chairman of the Inquiry. The first part will examine the culture, practices and ethics of the media. In particular, Lord Justice Leveson will examine the relationship of the press with the public, police and politicians. He is assisted by a panel of six independent assessors with expertise in key issues being considered by the Inquiry.203

The Inquiry has been established under the Inquiries Act 2005 and has the power to summon witnesses. It is expected that a range of witnesses, including newspaper reporters, management, proprietors, police officers and politicians of all parties will give evidence under oath and in public. It will make recommendations on the future of press regulation and governance consistent with maintaining freedom of the press and ensuring the highest ethical and professional standards.204

Lord Justice Leveson opened the hearings on 14 November 2011, saying:

[T]he press provides an essential check on all aspects of public life. That is why any failure within the media affects all of us. At the heart of this Inquiry, therefore, may be one simple question: who guards the guardians?205

No doubt freedom of speech and expression is the fundamental right of every human being and the primary duty of the media is to disseminate the news for public well being. But the above said burning issue has shocked the world and everyone has started believing that the media is over-reaching its powers under the protective shield of investigative journalism. In another sense, it amounts to intrusion into the private lives of individuals.

In the Leveson Inquiry, a wide range of witnesses, including newspaper reporters, management, proprietors, police officers and politicians of all parties, all gave evidence to the Inquiry under oath and in public. Part 1 of the Inquiry examined the culture, practices and ethics of the press and, in particular, the relationship of the press with the public, police and politicians.

203 http://www.levesoninquiry.org.uk/ accessed on February 29, 2012 at 6:05 IST
204 Ibid.
205 Ibid.
Lord Justice Leveson was assisted by a panel of six independent assessors with expertise in the key issues that were considered. Lord Justice Leveson published his Report on Part 1 of the Inquiry on 29 November 2012. Part 2 of the Inquiry cannot commence until the current police investigations and any subsequent criminal proceedings have been completed.\(^{206}\)

Justice Leveson found that the current systems of both internal governance in some parts of the press, and industry self-regulation of the press, have not worked and are not working.\(^{207}\) The present Press Complaints Commission (PCC) lacks the independence that is critical to building public confidence in a regulator.\(^{208}\) Justice Leveson envisaged that the industry should come together to create, and adequately fund, an independent regulatory body, headed by an independent Board, that would: set standards, both by way of a code and covering governance and compliance; hear individual complaints against its members about breach of its standards and order appropriate redress; take an active role in promoting high standards, including having the power to investigate serious or systemic breaches and impose appropriate sanctions; and provide a fair, quick and inexpensive arbitration service to deal with any civil complaints about its members’ publications.\(^{209}\) Justice Leveson further recommended that the standards code must ultimately be the responsibility of, and adopted by, the Board advised by a Code Committee which may comprise both independent members of the Board and serving editors. It was, therefore, recommended that the Code must take into account the importance of freedom of speech, the interests of the public (including the public interest in detecting or exposing crime or serious impropriety, protecting public health and safety and preventing the public from being seriously misled) and the rights of individuals. Specifically, it must cover standards providing for: (a) conduct, especially in relation to the treatment of other people in the process of obtaining material; (b) appropriate respect for privacy where there is no sufficient public interest justification for breach; and (c) accuracy, and the need to avoid misrepresentation.\(^{210}\)

It is further recommended that the Board should have the power to direct appropriate remedial action for breach of standards and the publication of corrections and apologies. Although remedies are essentially about correcting the record for individuals, the power to

\(^{206}\) <http://www.levesoninquiry.org.uk/> accessed on July 19, 2013 at 1:30 p.m. IST.


\(^{208}\) Id., at 1749.

\(^{209}\) Id., at 1759.

\(^{210}\) Id., at 1763.
require a correction and an apology must apply equally in relation to individual standards breaches (which the Board has accepted) and to groups of people (or matters of fact) where there is no single identifiable individual who has been affected. Again, it is recommend that the Board should have the power to impose appropriate and proportionate sanctions (including financial sanctions up to 1% of turnover, with a maximum of £1 million) on any subscriber found to be responsible for serious or systemic breaches of the standards code or governance requirements of the body. The sanctions that should be available should include power to require publication of corrections, if the breaches relate to accuracy, or apologies if the breaches relate to other provisions of the code. Financial sanctions should be appropriate and proportionate.

The Board should provide an arbitral process in relation to civil legal claims against subscribers, drawing on independent legal experts of high reputation and ability on a cost-only basis to the subscribing member; it should not be difficult to provide such expertise, not only from those who have retired from the Bench but also from the most senior ranks of the legal profession. The process should be fair, quick and inexpensive, inquisitorial and free for complainants to use (save for a power to make an adverse order for the costs of the arbitrator if proceedings are frivolous or vexatious). The arbitrator must have the power to hold hearings where necessary but, equally, to dispense with them where it is not necessary. The process must have a system to allow frivolous or vexatious claims to be struck out at an early stage.

In any reconsideration of the powers of the Information Commissioner (or replacement body), power is given to that body to determine that membership of a satisfactory regulatory body, which required appropriate governance and transparency standards from its members in relation to compliance with data protection legislation and good practice, should be taken into account when considering whether it is necessary or proportionate to take any steps in relation to a subscriber to that body.

The inquiry has been specifically into the press, not into the media more generally. Broadcasters are regulated by the Office of Communications (Ofcom), which is backed by law. Other people publishing on the internet, such as bloggers and tweeters, are not regulated as such, but are covered by laws on issues such as libel and contempt of court. Some, including MPs and

211 Id., at 1766.
212 Id., at 1767.
213 Id., at 1768-1769.
214 Id., at 1770.

159
peers, have questioned the wisdom of bringing more regulation to the press and not the wider internet. Lord Justice Leveson himself referred to material on the internet as ‘the elephant in the room’. However, any publisher could sign up to the new legislation-backed self regulator that Lord Justice Leveson envisages.215

Prime Minister David Cameron had reportedly promised to implement the recommendations, providing they were not ‘bonkers’. But within hours of the report’s publication, he said that he was not convinced legislation underpinning self-regulation was right. Mr. Cameron then warned the press the ‘the clock is ticking’ for them to introduce a self-regulation system with the tough powers set out by Lord Justice Leveson. "That means million-pound fines, proper investigation of complaints, prominent apologies," he said. Deputy Prime Minister Nick Clegg says he backs Leveson, highlighting a split within the coalition government. Labour leader Ed Miliband has urged the government to accept the report in its entirety.216

As the researcher observed that the right to privacy has been recognized in all civilized legal systems of the world. Since business process outsourcing is on rise, the European Union’s directives for protecting data privacy should be implemented in India. Similarly, Justice Leveson’s recommendations should also be implemented in India in order to regulate freedom of media.

---


216 Ibid.