APPENDIX

EXPANDING HORIZONS OF RIGHT TO PRIVACY: A STUDY

Questionnaire

Information about the respondent

Name : 
Address : 
Age : 
Gender : 
Occupation : 
Organization : 
E-mail : 

1. Do you know the meaning of ‘Privacy’?
   (a) Yes. (b) Somewhat. (c) No.
   If yes, please express your views:
   ...........................................................................................................
   ...........................................................................................................
   ...........................................................................................................
   ...........................................................................................................

* The names and the information provided herein will be kept strictly confidential and the information will be used only for analysis purposes for the research work- Lakhwinder Singh
2. Do you know about ‘Right to Privacy’?
   (a) Yes.   (b) Somewhat.   (c) No.

3. Do you agree that Right to Privacy is necessary for every human being?
   (a) Yes.   (b) No.   (c) Not Aware.

4. Do you know that Right to privacy is a part of Right to Life and Personal Liberty under Article 21 of the Indian Constitution?
   (a) Yes.   (b) Somewhat.   (c) No.

5. Do you know that Right to Privacy is not an absolute right and, can be restricted on some grounds?
   (a) Yes.   (b) Somewhat.   (c) No.
   If yes, please name any ground of restriction-

6. Do you know about ‘Right to Information’?
   (a) Yes.   (b) Somewhat.   (c) No.

7. Do you know that Right to Information for public purpose is an exception to the Right to Privacy?
8. Do you know that Freedom of Speech and Expression is a Fundamental Right under Article 19(1)(a) of the Indian Constitution?
   (a) Yes.  (b) Somewhat.  (c) No.

9. Do you know that Freedom of media is a part of Freedom of Speech and Expression?
   (a) Yes.  (b) Somewhat.  (c) No.

10. Do you know that Freedom of Media can be reasonably restricted on the ground of Right to Privacy?
    (a) Yes.  (b) Somewhat.  (c) No.

11. Do you agree that Investigative Reporting is a part of Freedom of Press?
    (a) Yes.  (b) No.  (c) Not Aware.

12. Do you agree that continuous broadcasting of sting operations creates a widespread public perception of the guilt of the accused and, it might also influence the decision of a trial court judge before whom the matter is pending?
    (a) Yes.  (b) No.  (c) Not Aware.

13. Do you agree that TV Reality show like ‘Emotional Atiyachaar’ on UTV Bindas exceeds the limit of decency by testing the loyalty of one’s boyfriend or girlfriend?
    (a) Yes.  (b) No.  (c) Not Aware.

14. Do you agree that there are sufficient measures to regulate sting operations?
    (a) Yes.  (b) No.  (c) Not Aware.

15. If aware, kindly share your viewpoints on ‘sting operations’.

   ........................................................................................................................................
   ........................................................................................................................................
16. Do you agree that celebrities enjoy less privacy than other individuals because of media’s over-inquisitiveness?
   (a) Yes.   (b) No.   (c) Not Aware.

17. Please, share your viewpoints on Celebrity’s Privacy?

18. Do you agree that self regulatory mechanism, i.e. code of ethics for media persons, is the best alternative than any other law to regulate freedom of Media?
   (a) Yes.   (b) No.   (c) Not Aware.

19. Do you agree that over-reaching powers of new media violate one’s right to privacy?
   (a) Yes.   (b) No.   (c) Not Aware.

20. Do you like someone unnecessarily talking about your private or personal matters?
   (a) Yes.   (b) No.   (c) Can’t Say.

21. Do you agree that in the age of new media and technology, people are capturing embarrassing private videos and pictures of each other and then, uploading them on the internet?
   (a) Yes.   (b) No.   (c) Not Aware.

22. Do you have an account on any social networking sites?
(a) Yes.  (b) No.  (c) Not Aware.

If yes, please answer following:

(i) Do you care about yours privacy settings at social networking sites like Facebook, MySpace, Orkut, etc.?

......................................................................................................................................................

(ii) Are you satisfied with Facebook or other social networking sites’ privacy settings?

......................................................................................................................................................

(iii) Have you ever felt that your privacy is being violated at social networking sites?

......................................................................................................................................................

23. Kindly, share your viewpoints on social networking sites?

......................................................................................................................................................
......................................................................................................................................................
......................................................................................................................................................
......................................................................................................................................................
......................................................................................................................................................
......................................................................................................................................................

24. Do you know about ‘Cyber Crimes’?

(a) Yes.  (b) Somewhat.  (c) No.

If yes, do you agree that present laws are not sufficient to tackle cyber crimes?

(a) Yes.  (b) Somewhat.  (c) No.

25. Do you agree that internet has become easily accessible to children?
26. Do you agree that children’s easy access to illegal websites affects their psychological privacy?
   (a) Yes.   (b) No.   (c) Not Aware.

27. Kindly, share your viewpoints regarding the impact of internet on children.

   ..........................................................................................................................
   ..........................................................................................................................
   ..........................................................................................................................
   ..........................................................................................................................
   ..........................................................................................................................

28. Do you agree that excessive surveillance violates one’s Right to Mental Privacy?
   (a) Yes.   (b) No.   (c) Not Aware.

29. Do you agree that after 26/11 Mumbai attacks governments’ surveillance power has been increased?
   (a) Yes.   (b) No.   (c) Not Aware.

30. Do you agree that the Government of India asks very personal questions in the Census Survey?
   (a) Yes.   (b) No.   (c) Not Aware.

31. Do you agree that Biometric Identification in Aadhaar number i.e. Unique Identification number is also one of the modes of governments’ surveillance power?
   (a) Yes.   (b) No.   (c) Not Aware.

32. Do you know that the Government can tap our phones and, intercept our e-mail IDs, social networking sites’ profiles, etc. for the security of the nation or public order or for the investigation of any offence?
(a) Yes.  (b) Somewhat.  (c) No.

If yes, do you agree that such power should be vested in the Government?

(a) Yes.  (b) Somewhat.  (c) No.

33. Do you agree that the government might use the surveillance methods for political purposes like taking revenge from opponents, dissenters, etc.?

(a) Yes.  (b) No.  (c) Not Aware.

34. Do you agree that excessive surveillance causes mental stress and manipulates individuals’ psychology, thoughts, and ideas?

(a) Yes.  (b) No.  (c) Not Aware.

35. Do you agree that people provide information to the government because they have complete trust in the government’s action of surveillance and interception?

(a) Yes.  (b) No.  (c) Not Aware.

36. Kindly, share your viewpoints on Government’s power of surveillance?

..........................................................................................................................
..........................................................................................................................
..........................................................................................................................

37. Do you know about Radio Frequency Identification (RFID) devices and Global Positioning System (GPS) technology?

(a) Yes.  (b) Somewhat.  (c) No.

If yes, do you agree that use of RFID radio-collars fitted with GPS technology as part of electronic surveillance by authorities, is a violation of individuals’ mental privacy?

(a) Yes.  (b) Somewhat.  (c) No.

38. Do you agree that unreasonable search and seizure by law enforcement agencies is a violation of one’s right to privacy under Indian Constitution?
39. Do you know that the Constitution of India recognizes the Rights of the Accused persons?
   (a) Yes. (b) Somewhat. (c) No.

   If yes, do you agree that the Police violate the rights of the accused persons?
   (a) Yes. (b) Somewhat. (c) No.

40. Do you know about misuses of DNA tests?
   (a) Yes. (b) Somewhat. (c) No.

   If yes, do you agree that every DNA test should be conducted only after obtaining the permission of a court?

41. Do you know about Narco analysis, Polygraph or lie detection tests?
   (a) Yes. (b) Somewhat. (c) No.

   If yes, do you agree that the authorized persons might misuse the Narco analysis tests by asking irrelevant, personal, indecent or obscene questions to the subject?

42. Do you know about a recent case in which the Hon'ble Supreme Court of India held that involuntary administration of Narco-analysis test is violative of one’s mental privacy?
   (a) Yes. (b) Somewhat. (c) No.

43. Do you agree that frisking or pat down search at shopping malls, Airports, etc. is an inhuman and indecent act and, violates our right to privacy?
   (a) Yes. (b) No. (c) Not Aware.

44. Do you know that Technological Scanners, which can see our naked bodies, are being monitored by human agents at Airports, Railway Stations, Shopping Malls, etc.?
(a) Yes.  (b) Somewhat.  (c) No.

If yes, do you agree that the technological scanners at Airports or Railway Stations or Bus Stands should show the image of contraband, weapons, etc. only and, not complete nude body?

(a) Yes.  (b) Somewhat.  (c) No.

45. Do you agree that spying capacity of CCTV and miniature hidden cameras, is being used by people frequently?

(a) Yes.  (b) No.  (c) Not Aware.

46. Do you agree that by installing Closed Circuit Television (CCTV) cameras at every public and private space, the crime has been reduced?

(a) Yes.  (b) No.  (c) Not Aware.

47. Do you agree that CCTV cameras have been installed at various places like shops, restaurants, shopping malls, etc. in an unregulated way; showrooms usually install miniature hidden cameras in Trial Rooms and; the camera control operators record videos for their personal use or to satisfy their erotic desires?

(a) Yes.  (b) No.  (c) Not Aware.

48. Do you agree that there are insufficient regulations regarding CCTV and miniature hidden cameras?

(a) Yes.  (b) No.  (c) Not Aware.

49. Please, share your views on CCTV cameras surveillance.
50. Do you agree that Telecom Service Providers like Airtel, Vodafone, Idea, etc. seek excessively personal information from subscribers at the time of SIM card registration?

(a) Yes.    (b) No.    (c) Not Aware.

51. Do you agree that Telecom Service Providers like Airtel, Vodafone, Idea, etc., usually disclose the personal information of their subscribers to any person?

(a) Yes.    (b) No.    (c) Not Aware.

52. Do you agree that business organizations share consumers’ personal information with each other for target marketing?

(a) Yes.    (b) No.    (c) Not Aware.

53. Do you feel disturbance when you receive messages regarding advertisements on your mobile phone?

(a) Yes.    (b) Somewhat.    (c) No.

54. Customers (landline and mobile) who do not want to receive commercial communications can dial or SMS to 1909 (toll free). Are you aware of this service?

(a) Yes.    (b) Somewhat.    (c) No.

55. Do you agree that Information Technology Act, 2000, and Credit Information Companies (Regulation) Act, 2005 are insufficient laws to protect Data Privacy in India?

(a) Yes.    (b) No.    (c) Not Aware.

56. Do you agree that employers collect information about employees' activities or lifestyle on the job and off the job?

(a) Yes.    (b) No.    (c) Not Aware.

57. Do you agree that employers should be free to conduct Psychological tests, DNA tests, etc. for all new job applicants?

(a) Yes.    (b) No.    (c) Not Aware.

58. Kindly, share your viewpoints on employees' privacy.
59. Do you agree that laws relating to right to privacy are insufficient?
   (a) Yes.   (b) No.   (c) Not Aware.

60. Kindly, suggest some measures for the protection of Right to Privacy?
Chapter 1.


[C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79]

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;


RECOGNISING that Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information;

RECOGNISING that more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks;

RECOGNISING that the continuous flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border co-operation among privacy enforcement authorities;
RECOGNISING the importance of risk assessment in the development of policies and safeguards to protect privacy;

RECOGNISING the challenges to the security of personal data in an open, interconnected environment in which personal data is increasingly a valuable asset;

DETERMINED to further advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among them;

On the proposal of the Committee for Information, Computer and Communications Policy:

I. RECOMMENDS that Member countries:

- Demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest levels of government;
- Implement the Guidelines contained in the Annex to this Recommendation, and of which they form an integral part, through processes that include all relevant stakeholders;
- Disseminate this Recommendation throughout the public and private sectors;

II. INVITES non-Members to adhere to this Recommendation and to collaborate with Member countries in its implementation across borders.

III. INSTRUCTS the Committee for Information, Computer and Communication Policy to monitor the implementation of this Recommendation, review that information, and report to the Council within five years of its adoption and thereafter as appropriate.

This Recommendation revises the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58/FINAL].
Annex

Guidelines governing the protection of privacy and transborder flows of personal data

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:
   a) “Data controller” means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.
   b) “Personal data” means any information relating to an identified or identifiable individual (data subject).
   c) “Laws protecting privacy” means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines.
   d) “Privacy enforcement authority” means any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings.
   e) “Transborder flows of personal data” means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties.

3. The principles in these Guidelines are complementary and should be read as a whole. They should not be interpreted:
   a) as preventing the application of different protective measures to different categories of personal data, depending upon their nature and the context in which they are collected, stored, processed or disseminated; or
b) in a manner which unduly limits the freedom of expression.

4. Exceptions to these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:
   a) as few as possible, and
   b) made known to the public.

5. In the particular case of federal countries the observance of these Guidelines may be affected by the division of powers in the federation.

6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
   a) with the consent of the data subject; or
   b) by the authority of law.
Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. Individuals should have the right:
   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
   b) to have communicated to them, data relating to them
      i. within a reasonable time;
      ii. at a charge, if any, that is not excessive;
      iii. in a reasonable manner; and
      iv. in a form that is readily intelligible to them;
   c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
   d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.
PART THREE. IMPLEMENTING ACCOUNTABILITY

15. A data controller should:
   a) Have in place a privacy management programme that:
      i. gives effect to these Guidelines for all personal data under its control;
      ii. is tailored to the structure, scale, volume and sensitivity of its operations;
      iii. provides for appropriate safeguards based on privacy risk assessment;
      iv. is integrated into its governance structure and establishes internal oversight mechanisms;
      v. includes plans for responding to inquiries and incidents;
      vi. is updated in light of ongoing monitoring and periodic assessment;
   b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and
   c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

PART FOUR. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

16. A data controller remains accountable for personal data under its control without regard to the location of the data.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.
PART FIVE. NATIONAL IMPLEMENTATION

19. In implementing these Guidelines, Member countries should:
   a) develop national privacy strategies that reflect a co-ordinated approach across governmental bodies;
   b) adopt laws protecting privacy;
   c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;
   d) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
   e) provide for reasonable means for individuals to exercise their rights;
   f) provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;
   g) consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy;
   h) consider the role of actors other than data controllers, in a manner appropriate to their individual role; and
   i) ensure that there is no unfair discrimination against data subjects.

PART SIX. INTERNATIONAL CO-OPERATION AND INTEROPERABILITY

20. Member countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.

21. Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.

22. Member countries should encourage the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.

23. Member countries should make public the details of their observance of these Guidelines.
Chapter 2.

Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)

Introduction

In 1980, the OECD adopted the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("1980 Guidelines") to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. The 1980 Guidelines, which contained the first internationally agreed-upon set of privacy principles, have influenced legislation and policy in OECD Member countries and beyond. Framed in concise, technology-neutral language, they have proven remarkably adaptable to technological and societal changes. Nevertheless, changes in personal data usage, as well as new approaches to privacy protection, have left the 1980 Guidelines in need of updating in a number of important respects. The Honourable Michael Kirby chaired the original OECD expert group that drafted the Guidelines. In reflecting on that achievement on the occasion of the Guideline’s 30th anniversary Justice Kirby observed: “In the field of information policy, the technology is such that no international expression of principles can be immune from the forces of change.”

Context of the review

Over the last three decades, personal data have come to play an increasingly important role in our economies, societies and everyday lives. Innovations, particularly in information and communication technologies, have impacted business operation, government administration, and the personal activities of individuals. New technologies and responsible data uses are yielding great societal and economic benefits. The volume of
personal data being collected, used and stored is vast and continues to grow. Modern communications networks support global accessibility and continuous, multipoint data flows. The potential uses of personal data have increased tremendously as a result of the wide range of analytics that can provide comprehensive insights into individuals’ movements, interests, and activities.

At the same time, the abundance and persistence of personal data have elevated the risks to individuals’ privacy. Personal data is increasingly used in ways not anticipated at the time of collection. Almost every human activity leaves behind some form of digital data trail, rendering it increasingly easy to monitor individuals’ behaviour. Personal data security breaches are common. These increased risks signal the need for more effective safeguards in order to protect privacy.

In recent years, several initiatives have been undertaken to address new and elevated privacy risks, particularly in the context of transborder data flows. The work is ongoing and examples include the European Union’s system of Binding Corporate Rules (BCRs); the global discussion on the commonly accepted elements of privacy accountability, and the Asia Pacific Economic Cooperation’s Cross-Border Privacy Rules System (APEC CBPR). At the OECD, cross-border co-operation among privacy enforcement authorities has been a priority, resulting in the adoption of the 2007 Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (the “2007 Recommendation”, [OECD, 2007]).

The Seoul Declaration for the Future of the Internet Economy (2008) recommended that the OECD assess the application of certain OECD instruments, including the 1980 Guidelines, in light of “changing technologies, markets and user behaviour and the growing importance of digital identities.” This Declaration triggered the launch of a formal review of the 1980 Guidelines.

The OECD Recommendation on Principles for Internet Policy Making (OECD, 2011a) called for a strengthening of consistency and effectiveness in privacy protection at a global level. While the OECD Privacy Guidelines have a broader scope than Internet policies, the 2011 Recommendation is nevertheless instructive. The Communiqué attached to the 2011 Recommendation for information purposes explains that current privacy challenges are likely to become more acute “as the economy and society depends more heavily on broadened and innovative uses of personal information that can be more easily gathered, stored, and analysed” (OECD, 2011b).
Privacy frameworks around the world are being examined and refined. Three of the primary frameworks with an international dimension (OECD, European Union, and Council of Europe) have been under review simultaneously, and a fourth (APEC) is implementing new cross-border arrangements. Work on domestic privacy frameworks is likewise underway across the globe, from Australia to Brazil to China to the United States. In light of all of these developments, the OECD concluded that it was an appropriate time to engage in a substantive review of the 1980 Guidelines.

Process of the review

Preparations for the review began in 2010, in the context of the 30th anniversary of the 1980 Guidelines. As part of the process, the OECD organised three thematic events. These events addressed (1) the impact of the 1980 Guidelines; (2) the evolving role of the individual; and (3) the economic dimensions of personal data and privacy. It also produced two reports, “The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines” (OECD, 2011c), and “Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation” (OECD, 2011d).

Building on this preparatory work, the Working Party for Information Security and Privacy (WPISP) developed Terms of Reference (OECD, 2011e) to serve as a roadmap for the review. The Terms of Reference articulated a shared view of current issues and approaches, and provided the rationale for further work. In addition to highlighting the changes in the environment, the Terms of Reference identified those elements which Member countries considered essential to improving the effectiveness of privacy protections.

A Volunteer Group of Privacy Experts (“Expert Group”) was formed to assist the WPISP in the review process. This group included experts from governments, privacy enforcement authorities, academics, business, civil society, and the Internet technical community. Participants also included representatives of the Council of Europe and the European Union, as well as experts active in APEC. This multi-stakeholder group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada. Omer Tene served as the Rapporteur to the group. The Expert Group collaborated through a series of meetings and a virtual workspace during 2011 and 2012. During these meetings, the Expert Group focused on three main themes identified by the Terms of Reference, namely: (1) the roles and responsibilities of key actors; (2) geographic restrictions on transborder data flows; and (3) proactive implementation and enforcement.
The approach that emerged from the work of the Expert Group suggested that, although the environment for privacy and transborder data flows has changed significantly, an update to the 1980 Guidelines was preferred rather than a fundamental rethinking of its core principles. The Expert Group took the view that the balance reflected in the eight basic principles of Part Two of the 1980 Guidelines remains generally sound and should be maintained. The Expert Group introduced a number of new concepts to the OECD privacy framework, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other aspects of the 1980 Guidelines were expanded or updated, such as accountability, transborder data flows and privacy enforcement.

The 1980 Guidelines were accompanied by an Explanatory Memorandum, which described the environment that led to their development, as well as their underlying rationale. The Explanatory Memorandum provides insight into the competing priorities of the time, as well as a detailed interpretation of various provisions in the 1980 Guidelines, some of which have not been modified (in particular those of Part Two). These insights remain relevant today. This Supplementary Explanatory Memorandum has been prepared as part of the review process to complement the revised Guidelines. It is intended to supplement – not replace – the original Explanatory Memorandum. Where there have been changes to the 1980 Guidelines, this Supplementary Explanatory Memorandum sheds light on the rationale and context of these changes to help understand and interpret them.
Revisions to the Guidelines

Privacy management programmes

Part Two of the 1980 Guidelines sets forth the principle of accountability, which places the onus on the data controller to comply “with measures that give effect to the rest of the principles”. Recognition of the importance of the accountability principle has increased over time. Domestic privacy laws have come to introduce a variety of mechanisms designed to promote the accountability of both public and private data controllers. Obligations of transparency towards individuals and privacy enforcement authorities are clear examples of such mechanisms.

In recent years, the principle of accountability received renewed attention as a means to promote and define organisational responsibility for privacy protection. Building on this experience, the new Part Three of the Guidelines (“Implementing Accountability”) introduces the concept of a privacy management programme and articulates its essential elements.

Paragraph 15(a)(i) specifies that a data controller’s privacy management programme should give effect to the Guidelines “for all personal data under its control”. The term “control” refers back to the definition of a “data controller”, as defined in paragraph 1(a). This formulation emphasises that a privacy management programme should not only address the data controller’s own operations, but all operations for which it may be accountable - regardless of to whom data is transferred. For example, a privacy management programme should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf: Safeguards may also be necessary in relationships with other data controllers, particularly where the responsibility for giving effect to the Guidelines is shared. Appropriate safeguards may include: provisions in contracts that address compliance with the data controller’s privacy policies and practices; protocols for notifying the data controller in the event of a security breach; employee training and education; provisions for sub-contracting; and a process for conducting audits.
Paragraph 15(a)(i) refers only to the Guidelines as a source of rules or principles to be implemented through a privacy management programme. In practice, privacy management programmes may need to reflect other sources as well; including domestic law, international obligations, self-regulatory programmes, or contractual provisions.

Paragraph 15(a)(ii) underlines the need for flexibility when putting in place a privacy management programme. For example, large data controllers with locations in multiple jurisdictions may need to consider different internal oversight mechanisms than small or medium sized data controllers with a single establishment. At the same time, paragraph 15(a)(ii) also provides that privacy management programmes should be adapted to the volume and sensitivity of the controller’s operations. Programmes for data controllers that deal with large volumes of personal data will need to be more comprehensive than those of data controllers who handle only limited amounts of personal data. The sensitivity of the data controller’s operations may also impact the nature of a privacy management programme, as even a very small data controller may handle extremely sensitive personal data.

A recurring element in the discussions about privacy management programmes was the need for such programmes to develop appropriate safeguards based on privacy risk assessment. Paragraph 15(a)(iii) contemplates that the determination of the necessary safeguards should be made through a process of identifying, analysing and evaluating the risks to individuals’ privacy. This process is sometimes accomplished by conducting a “privacy impact assessment” before a new programme or service is introduced or where the context of the data use changes significantly. “Risk” is intended to be a broad concept, taking into account a wide range of possible harms to individuals. A privacy management programme can also assist in the practical implementation of concepts such as “privacy by design”, whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an afterthought.

Paragraph 15(a)(iv) indicates that privacy management programmes should be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms. Obtaining support and commitment from senior management is a key factor in ensuring the successful implementation of a privacy management programme. Ensuring the availability of sufficient resources and staff, as well as training programmes, may also improve the effectiveness of the programme. Privacy officers may play an important role in designing and implementing a privacy management programme.
Paragraph 15(a)(v) provides that a privacy management programme should also include plans for responding to incidents and inquiries. The increasing frequency of security breaches affecting personal data demonstrates the importance of developing an incident response plan, which includes breach notification (see below). To support the “Individual Participation Principle” in Part Two, data controllers should also be able to provide timely response to inquiries (either in the form of complaints or requests for information) by data subjects. Finally, paragraph 15(a)(vi) stipulates that privacy management programmes should be routinely reviewed and updated to ensure that they remain appropriate to the current risk environment.

Paragraph 15(b) provides that a data controller should be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines. Establishing the capacity and effectiveness of a privacy management programme, even in the absence of a personal data security breach or allegation of non-compliance, enhances the accountability of data controllers. The assessment of the programme may be carried out directly by the privacy enforcement authority or by an agent on its behalf.

Paragraph 15(b) includes the terms “appropriate” and “competent” to highlight that data controllers should be prepared to demonstrate their privacy management programmes at the request of a privacy enforcement authority provided that this authority has jurisdiction over the data controller. The Guidelines do not address legal issues related to jurisdiction, competence and conflicts of law.

A privacy management programme may also be demonstrated to an entity which is responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to Guidelines. Such arrangements may involve seal programmes or certification schemes, and may also concern transborder flows of personal data. In this regard it can be noted that paragraph 21 encourages the development of international arrangements that give practical effect to the Guidelines. The European Union’s Binding Corporate Rules (BCRs) and the APEC Cross-border Privacy Rules System provide two models for developing such an arrangement.
Data security breach notification

The “Security Safeguards Principle” of Part Two states that “Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.” Numerous high-profile data breaches have demonstrated that personal data security continues to be a challenge.

Data breaches can result, for example, from actions by careless employees who fail to follow proper procedures; hackers who gain access to inadequately protected databases; or opportunistic thieves who steal unsecured portable devices. However, the underlying causes - lack of employee training and awareness, out-of-date security safeguards, inadequate rules governing access to personal data, over-collection of data and undefined retention periods, or a lack of adequate oversight - can often be attributed to the data controller.

The potential harm to individuals from the misuse of their personal data, whether accidentally lost or purposefully stolen, may be significant. Organisations experiencing a breach often incur significant costs responding to it, determining its cause, and implementing measures to prevent recurrence. The reputational impact can also be significant. A loss of trust or confidence can have serious consequences for organisations. As a result, the security of personal data has become an issue of great concern to governments, businesses and individuals.

Breach notification laws requiring data controllers to inform individuals and/or authorities when a security breach has occurred have been passed or proposed in many countries. These laws are usually justified on the grounds that data controllers have little incentive to disclose breaches voluntarily, given the possible harm this can cause to their reputation. Requiring notification may enable individuals to take measures to protect themselves against the consequences of identity theft or other harms. Notification requirements may also provide privacy enforcement authorities or other authorities with information to determine whether to investigate the incident or take other action. Ideally, breach notification laws also help to create an incentive for data controllers to adopt appropriate security safeguards for the personal data they hold.

In addition to contributing to data security, data breach notification enhances other basic principles set forth in Part Two of the Guidelines, including accountability, individual participation and openness. Furthermore, mandatory security breach notification may improve the evidence base for privacy and information security policies by generating information about the number, severity and causes of security breaches.
Security breaches not only raise privacy concerns, but also intersect with other issues, including criminal law enforcement and cybersecurity. When an organisation suffers a security breach, particularly one resulting from an external attack, notification of the breach to authorities other than privacy enforcement authorities (e.g. computer incident response teams, criminal law enforcement entities, other entities responsible for cybersecurity oversight) may be appropriate or required.

Requiring notification for every data security breach, no matter how minor, may impose an undue burden on data controllers and enforcement authorities, for limited corresponding benefit. Additionally, excessive notification to data subjects may cause them to disregard notices. Accordingly, the new provision that has been added to the Guidelines reflects a risk-based approach to notification. Notice to an authority is called for where there is a “significant security breach affecting personal data”, a concept intended to capture a breach that puts privacy and individual liberties at risk. Where such a breach is also likely to adversely affect individuals, notification to individuals would be appropriate as well.

To determine whether individuals are likely to be “adversely affected” by a breach, the term “adverse effect” should be interpreted broadly to include factors other than just financial loss. Notification requirements should be flexible to allow for prevention and mitigation of further damage. There may be circumstances where notification to data subjects would be inappropriate, for example when it would increase the risk to data subjects or impede a law enforcement investigation.

Existing breach notification laws differ in terms of the thresholds for notification, the parties to be notified, the timing of the notification, as well as the role of privacy enforcement and other authorities. Further experience may be needed to determine which modalities of breach notification are most effective in practice.

Security breaches may affect the personal data of individuals residing in different jurisdictions. When designing, implementing or revising breach notification requirements, special consideration may be given to the interests of affected individuals who may live outside their jurisdiction. In particular, the notification of privacy enforcement authorities in other jurisdictions where a significant number of individuals are known or likely to have been affected, can be beneficial. Cross-border enforcement cooperation mechanisms are one way to foster arrangements that might support or disseminate breach notifications of importance to multiple jurisdictions. Such arrangements may also help to address issues arising from conflicting legal requirements.
Privacy enforcement authorities

Neither the 1980 Guidelines nor the 2007 Recommendation explicitly call for the establishment of privacy enforcement authorities, although the latter instrument assumes their existence and recommends their endowment with effective powers and authority. The revised Guidelines define and make explicit the need to establish and maintain “privacy enforcement authorities”. They also incorporate a definition of “laws protecting privacy”, to refer to “national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines”. Both definitions mirror those agreed in the 2007 Recommendation.

The definitions of “laws protecting privacy” and “privacy enforcement authorities” allow for flexibility in application. “Laws protecting privacy” can refer not only to horizontal privacy laws that are common in Member countries, but also to sectoral privacy legislation (e.g. credit reporting or telecommunications laws) or other types of legislation that contain provisions which protect personal data so as to give effect to the Guidelines in practice (e.g. consumer protection laws). Likewise, a “privacy enforcement authority” refers not only to those public sector entities whose primary mission is the enforcement of national privacy laws, but may for example also extend to regulators with a consumer protection mission, provided they have the powers to conduct investigations or bring proceedings in the context of enforcing “laws protecting privacy”.

A new provision in Part Five (“National Implementation”) calls on Member countries to establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an “objective, impartial and consistent basis” [paragraph 19(c)]. This formulation has been adapted from the 2012 OECD Recommendation on Regulatory Policy and Governance (OECD, 2012a). In the context of the Guidelines, it refers to the need for privacy enforcement authorities to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy. There exist a variety of mechanisms across Member countries for ensuring the necessary impartiality of privacy enforcement authorities in the exercise of their privacy protection functions. Paragraph 19(c) focuses on the practical impact of such mechanisms, which should ensure that these authorities can take decisions free from influences that could compromise their professional judgment, objectivity or integrity.
In some countries, the term “privacy enforcement authority” can also refer to a group of bodies that collectively enforce laws protecting privacy. For example, oversight of public sector data controllers may involve multiple bodies from different branches of government, who may also have the authority to issues guidelines or other data usage requirements. The “governance, resources, and technical expertise” called for in paragraph 19(c) may not, in such a case, be embodied in a single entity, but rather be found in the enforcement system as a whole.

The 2007 Recommendation underlined the need for privacy enforcement authorities to be endowed with the resources and authority necessary to (a) deter and sanction violations of laws protecting privacy; (b) permit effective investigations, including the ability to obtain access to relevant information, relating to possible violations of laws protecting privacy; and (c) permit corrective action to be taken against data controllers engaged in violations of laws protecting privacy. The resources of privacy enforcement authorities should be commensurate with the scale and complexity of data processing operations subject to their oversight. The new provision also calls for empowering privacy enforcement authorities with sufficient technical expertise, which has become crucial in light of the increasing complexity of data uses. This reinforces the emerging trend within privacy enforcement authorities to retain staff with a technical background.

**Transborder flows of personal data**

When the 1980 Guidelines were drafted, data flows largely constituted discrete point-to-point transmissions between businesses or governments. Today, data can be processed simultaneously in multiple locations; dispersed for storage around the globe; re-combined instantaneously; and moved across borders by individuals carrying mobile devices. Services, such as “cloud computing”, allow organisations and individuals to access data that may be stored anywhere in the world.

The 1980 Guidelines presumed that data flows should generally be allowed, but recognised the ability of governments to restrict them in certain circumstances, namely where the receiving country “does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation.” Since then, Member countries have instituted a range of mechanisms to ensure the protection of individuals in the context of transborder data flows. Some of these mechanisms include a country-specific assessment, such as the “adequacy model” adopted within the European Union. Other mechanisms are not based on a country-specific assessment, but are instead based on the safeguards put in place by data controllers. Such mechanisms include, for example, Binding Corporate Rules, model contracts, and Cross-Border Privacy Rules.
The revisions reflected in Part Four attempt to simplify and consolidate the OECD approach to transborder flows of personal data. It begins by recalling that a data controller remains accountable for personal data under its control without regard to the location of the data [paragraph 16]. This paragraph restates the basic principle of accountability contained in Part Two in the context of transborder data flows. Transborder flows of personal data, to Member countries or non-Member countries, present risks, which data controllers must address. Some data flows may require close attention because of the sensitivity of the data or because the receiving jurisdiction may lack either the willingness or capacity to enforce privacy safeguards.

Without precluding the application of paragraph 6, paragraph 17 specifies two circumstances in which a Member country should refrain from imposing restrictions on transborder flows of personal data. Paragraph 17(a) retains the general approach from the 1980 Guidelines, by providing that Member countries should refrain from restricting transborder data flows between itself and another country where the other country substantially observes these Guidelines. Paragraph 17(b) discourages restrictions where sufficient safeguards exist to ensure a continuing level of protection consistent with these Guidelines. It gives recognition to the measures which a data controller can put in place to ensure a continuing level of protection, which may result from a combination of measures, such as technical and organisational security safeguards, contracts, complaint handling processes, audits, etc. However, the measures provided by the data controller need to be sufficient and supplemented by mechanisms that can ensure effective enforcement in the event these measures prove ineffective. Paragraph 17(b) therefore includes as a consideration the availability of effective enforcement mechanisms which support measures adopted by the data controller. Such enforcement mechanisms may take a variety of forms, including for example, administrative and judicial oversight, as well as cross-border co-operation among privacy enforcement authorities.

Paragraphs 16 and 17 operate independently. The existence or absence of country restrictions on data flows adopted pursuant to paragraph 17 does not, as such, affect the operation of the principle embodied by paragraph 16, namely that data controllers remain accountable for personal data under their control, including in the context of transborder flows.

Paragraph 18 updates the language in the 1980 Guidelines to refer to “risk” and “proportionality”, indicating that any restrictions upon transborder data flows imposed by Member countries should be proportionate to the risks presented (i.e. not exceed the requirements necessary for the protection of personal data), taking into account the sensitivity of the data, the purpose and context the processing. In doing so, the text has been made more coherent with other provisions of the Guidelines, which implement a risk-based approach.

THE OECD PRIVACY FRAMEWORK © OECD 2013
Paragraph 6 of the Guidelines acknowledges that Member countries have the ability to supplement the standards set forth by the Guidelines with additional measures necessary for the protection of privacy and individual liberties, which may impact transborder flows of personal data. Such measures should be implemented in a manner that least impacts the free flow of personal data.

National implementation

Regarding national implementation, the 1980 Guidelines focused on the need for “legal, administrative and other procedures or institutions”. Although the 1980 Guidelines also highlighted non-regulatory measures, including self-regulation, it was recognised that there is a need for additional measures to help to protect privacy.

Paragraph 19(a) recommends that Member countries develop national privacy strategies that reflect a co-ordinated approach across governmental bodies. Elevating the importance of privacy protection to the highest levels within government helps improve the effectiveness of privacy protection. A further element of national privacy strategies concerns intra-governmental co-ordination. As highlighted in the OECD Recommendation on Regulatory Policy and Governance, Member countries should promote regulatory coherence between various levels of government. Where governments act as a policy maker for private sector activity, ensuring co-ordination across governmental departments is a necessary part of a national strategy. In addition, with many government departments making use of personal data, another dimension of co-ordination is to ensure a consistent level of protection across governmental bodies. Finally, national privacy strategies also offer a vehicle to ensure compatibility of policy development in related areas (e.g. national cybersecurity strategies).

Paragraph 19(g) calls upon Member countries to consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy. While existing initiatives attempt to raise awareness, there is broad recognition that more needs to be done. The Terms of Reference for the review of the Guidelines called for the creation of a culture of privacy among organisations and individuals through implementation of privacy literacy initiatives. Recent OECD instruments in related areas include measures for education and awareness as part of their policy frameworks. Such initiatives should involve a wide range of stakeholders, including governments, privacy enforcement authorities, self-regulatory bodies, civil society organisations, and educators. As children are a particularly vulnerable category of data subjects, Member countries are specifically...
encouraged to consider privacy literacy initiatives which seek to equip children with the knowledge and skills necessary to stay safe online and use the Internet to their benefit.

Privacy professionals play an increasingly important role in the implementation and administration of privacy management programmes. Several Member countries have already undertaken initiatives to define the competencies of privacy professionals. Credential programmes in data protection and privacy, as well as specialised education and professional development services may contribute to the development of the necessary skills. Paragraph 19(g) explicitly encourages Member countries to consider the adoption of measures to support such skills development.

Technical measures also play an increasingly important role in complementing laws protecting privacy. Paragraph 19(g) encourages measures to foster the development and deployment of privacy-respecting and privacy-enhancing technologies (PETs). For example, Member countries may choose to support the development of technical standards which advance privacy principles. International standardisation initiatives may also advance technical interoperability among PETs, which may in turn help promote wider adoption of these technologies. Accreditation and seal programmes may further foster the adoption of technologies beneficial to privacy. Other measures include the promotion of research and development, exchange of best practices, and the issuance of regulatory guidance.

Paragraph 19(h) invites Member countries to consider the role of actors other than data controllers, “in a manner appropriate to their individual role”. When discussing the need for complementary measures, it was recognised that other actors who, while not covered by the concept of data controller, nevertheless play an important role in determining the level of protection of personal data. Over the past few years, individuals have transcended the role of passive “data subjects” to become actively involved in creating, posting and sharing personal data about themselves, friends, relatives and others, over a vast array of information outlets including social networking services, rating systems and geo-location based applications. When discussing this change, it was recognised that not every actor should necessarily be regulated in the same way. For example, individuals acting in the context of their private lives are generally perceived to fall outside the remit of the Guidelines, as relationships among individuals are usually fundamentally different from those between individuals and organisations. Non-legislative measures, including education and awareness raising, were considered more appropriate to address the privacy risks associated with the activities of individuals. Where an individual does cause damage to the privacy interests of others, tort or civil law may offer a possible remedy, but other measures may need to be considered as well.
International co-operation and interoperability

The OECD Recommendation on Internet Policy Making calls for a strengthening of consistency and effectiveness in privacy protection at a global level. The Communiqué which is annexed to it for information purposes further recognises the objective of governments to pursue global interoperability in this area. The Terms of Reference similarly identified the value of globally interoperable privacy frameworks that ensure effective protection of privacy and support the free flow of personal information around the world. However, as outlined by the G8 Deauville Declaration, we still “face considerable challenges in promoting interoperability and convergence among our public policies on issues such as the protection of personal data” (G8, 2011).

Paragraph 21 expresses the general objective of Member countries to improve global interoperability of privacy frameworks through international arrangements that give practical effect to the Guidelines. There exists a range of approaches to interoperability among privacy frameworks. The US-EU Safe Harbour Framework6, which was adopted under the EU adequacy regime and implemented in 2000, was an early example. Since then, several initiatives have been undertaken to bring together different approaches and systems of protection, including work by the privacy enforcement authorities within the framework of the EU Binding Corporate Rules and the APEC Cross-Border Privacy Rules System within the Asia-Pacific region. At the time of publication of these revised Guidelines, the Council of Europe continues its deliberations on the modernisation of Convention 108 on the Automated Processing of Personal Data. Further work is needed at the policy level towards a more seamless approach to global privacy governance.

A strong global network of privacy enforcement authorities working together is a first important step towards global interoperability. In 2005, the OECD revisited the issue of global cooperation among privacy enforcement authorities, resulting in the adoption of a new framework for cross-border co-operation in the form of the 2007 Recommendation. The three-year implementation report for the 2007 Recommendation highlighted the need for further efforts to ensure that privacy enforcement authorities have sufficient powers to administer effective sanctions and resources to accomplish their mission. The Terms of Reference for the review of the Guidelines called for a redoubling of efforts to develop a globally active network of privacy enforcement authorities. Paragraph 20 reiterates the commitment expressed by Member countries in the 2007 Recommendation to enhance co-operation between privacy enforcement authorities. In particular, Member countries are encouraged to address obstacles – be they
legal or practical – towards information sharing among privacy enforcement authorities to facilitate coordinated and effective enforcement. Reducing the barriers to information sharing has been a particular concern in this respect.

Improving the global interoperability of privacy frameworks raises challenges but has benefits beyond facilitating transborder data flows. Global interoperability can help simplify compliance by organisations and ensure that privacy requirements are maintained. It can also enhance individuals’ awareness and understanding of their rights in a global environment.

Improving the evidence base for policy making

The OECD Recommendation on Internet Policy Making calls for the development of capacities to bring publicly available, reliable data into the policy-making process. The Communiqué, annexed to it for information, specifically notes the value of internationally comparable metrics.

The evidence base which is currently available for policymaking in the area of privacy is uneven. Household surveys by national statistical agencies provide some insight into privacy issues on the basis of internationally comparable metrics. However, the scope of these surveys, which focus primarily on awareness issues among individuals, is limited. There are gaps, for example, related to the technical or economic dimensions of privacy, as well as the implementation of prevention measures. Privacy enforcement authorities gather considerable data that are made public through annual reports, but not in a format well-suited to international comparisons. For example, progress in understanding complaint data, data breach statistics, and how fines and other sanctions influence data controllers’ behaviour could be a potentially rich source of insight for policy makers. The addition of paragraph 22 in Part Six identifies the need for Member countries’ support for initiatives to improve the evidence base in this area.

Other updates

In addition to the substantive changes discussed in the previous section, the revised Guidelines reflect several minor changes which were made either to enhance readability or otherwise update the language of the 1980 Guidelines.

As a general matter, all references to specific parts of the Guidelines, have been replaced by a more generic phrasing (“these Guidelines”).
Paragraph 2, which specifies the scope of the Guidelines, now refers to a “risk” rather than “danger” to privacy and individual liberties, reflecting the increased emphasis on risk within the revised Guidelines. This change should not be construed as preventing Member countries from extending the scope of laws protecting privacy or other privacy regimes to all forms of processing of personal data.

Former paragraph 3(b) has been deleted, as the ability for Member countries to exclude from the application of the Guidelines “personal data which do not pose any risk to privacy and individual liberties” is already reflected in paragraph 2.

Former paragraph 3(c) has been deleted, as Member countries have generally extended the scope of their domestic privacy laws to include the processing of personal data in general.

A new paragraph 3(b) has been added, to recognise the potential conflict between the protection of privacy and other fundamental rights arising from the now ubiquitous nature of personal data processing. It is also in line with the Communiqué on Principles for Internet Policy Making (OECD, 2011g) which underlines that "[p]rivacy rules should also consider the fundamental rights of others in society including rights to freedom of speech, freedom of the press, and an open and transparent government”.

Former paragraphs 15 and 16 of the 1980 Guidelines were removed in the interests of clarity and to avoid repetition, as the commitment of Member countries to the global free flow of information and security is already underlined elsewhere in the Recommendation.
Notes


2. The system of BCRs is being further developed, see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm


7. See OECD (2011f).
References


THE MOBILE CAMERA PHONE USERS (CODE OF CONDUCT) BILL, 2006

A BILL to provide for a code of conduct for users of mobile camera phones at certain places including public places; to regulate their use by children; to assign responsibilities on the user to respect the privacy of others and matters connected therewith or incidental thereto.

Be it enacted by Parliament in the Fifty-seventh Year of the Republic of India as follows:—

1. (1) This Act may be called the Mobile Camera Phone Users (Code of Conduct) Act, 2006.

(2) It extends to the whole of India.

(3) It shall come into force with immediate effect.

2. In this Act, unless the context otherwise requires,—

(a) “camera phone” means and includes any mobile telephone capable of recording video as well as the still photographs;

(b) “child” means a person who has not completed eighteen years of age;

(c) “objectionable content” means taking photograph or video of unclothed body or part of body of a person with or without his knowledge;
Restriction on use of camera phones in public and other places.

Restrictions on use of camera phones in defence and other establishments.
Prohibition of use of camera phone by children.

Camera phones to flash light or emit sound while taking photo or recording video.

Central Government to restrict use of camera phones.

Camera phone user to respect the privacy of others.

Manufacturing companies educate to retailers.

Central Government to frame mobile camera phone policy.

Penalty.

(d) “prescribed” means prescribed by rules made under this Act;

(e) “public place” means any place being frequently visited by the public at large and includes government buildings, hospitals, banks, markets, restaurants, clubs, hotels, parks, monuments, libraries, museums and other like places but does not include private residence or gathering;

(f) “public transport” means taxis, buses, trams, rails, ships including other vessels of similar kind, aeroplanes run by government or private sector for the use of general public.

3. (1) No person shall use camera phone to take photograph or record video of any other person without his knowledge or consent in any public place or public transport.

(2) No person shall use camera phone,—

(i) where photography is specifically prohibited; and

(ii) while driving a motor vehicle.

4. No person shall carry or use camera phone in high security defence establishments, and such other establishments as the Central Government may, by notification in the Official Gazette, declare in order to prevent sensitive information or topography being snapped or leaked.

5. (1) No child shall be allowed to possess or use a camera phone.

(2) If any child is caught with a camera phone, his parents or any person who, at that time, is the guardian of the child shall be prosecuted in accordance with the provisions of this Act.

6. (1) On and from the appointed day, as the Central Government may appoint in this behalf, no person shall carry or use a camera phone, which does not flash a light or emit sound of a prescribed decibel on taking photograph/recording video.

(2) It shall be the responsibility of every phone company to manufacture only such camera phones which comply with the requirements of sub-section (1) and ensure that there is no provision to disable these features in camera phones.

7. The Central Government may, by notification in the Official Gazette, restrict the use of camera phones in such areas, as it may deem necessary in the public interest.

8. It shall be the responsibility of the person using the camera phone to respect the privacy of other and no person shall use the camera phone for shooting and circulating objectionable content.

9. It shall be the responsibility of the company manufacturing the camera phones to educate the retailer to actively apprise the customers about the appropriate and ethical use of camera phone at the time of purchase.

10. The Central Government shall within six months of the commencement of this Act, shall frame a mobile camera phone policy.

11. Whoever contravenes the provisions of this Act and rules made thereunder shall be punishable with imprisonment which may extend to three years or with fine which may extend to twenty-five thousand rupees or with both:

Provided that if the contravention of the provisions of the Act, and the rules is done by a company, the fine may extend to twenty-five lakhs.
12. (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.— For the purpose of this section:

(i) “company” means anybody corporate and include a firm or other association of individuals; and

(ii) “director”, in relation to a firm, means a partner in the firm.

13. Notwithstanding anything contained in the Code of Criminal Procedure 1973, the offence under this Act shall be cognizable.

14. All offences under this Act shall be tried summarily in the manner prescribed for summary trial under the Code of Criminal Procedure 1973.

15. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions, not inconsistent with the provisions of this Act, as appear to it to be necessary or expedient for removing the difficulty:

Provided that no such orders shall be made after the expiry of the period of three years from the date of commencement of this Act.

16. The provisions of this Act shall be in addition to, and not in derogation of, the provisions in any other law, for the time being in force, relating to mobile camera phones.

17. The Central Government may by notification in the Official Gazette, make rules for carrying out the purposes of this Act.
STATEMENT OF OBJECTS AND REASONS

There is a quantum jump in the number of mobile camera phone users in the world. The sale of camera phones has outnumbered the sale of stand-alone digital cameras. Our country is no exception to this boom in the users of camera phones. The number of mobile camera phone users is increasing at a tremendous speed along with its misuse. People are secretly taking photographs of women without their knowledge and consent. At times, intimate and private images of women are taken to harass or blackmail them, since photo snapped with these cameras can be transmitted instantly to other cell phones, to e-mail and even to web.

Digital shoplifting by these camera phones is another area of concern. In many places in the world, people are not buying books and magazines as they are snapping them free from the shops using camera phones. Many bookstores have banned the use of camera phone to shoot pages from periodicals instead of buying them as it has a devastating effect on their sales. The corporate espionage has become easy by camera phone as any disgruntled employee can snap and transmit photo of a product development/specifications of product or secret ingredients and destroy the business. Camera phones present a number of risks to intellectual property, trade secrets and other confidential business operations of companies. Customer information can be easily and surreptitiously caught on a camera phone and passed on to other interested parties. One camera phone manufacturing company, has itself banned the use of this phone in their semiconductor and research facilities to stave off industrial espionage.

Another area of concern is the use of camera phones in places where photography is prohibited. People smuggle in small camera phones and take the pictures of various artefacts in museums or in religious places. Use of camera phone can also cause trouble in defence establishments or high security establishments.

Further, camera phone in the hands of students can also be misused by them. There is no need for a child to have a camera phone. At the most, he can be given a cell phone.

The need of the hour is that the Government should come forth and frame a national camera phone policy. In Europe, some gyms and swimming pools have banned camera phone in changing room. In Japan, Singapore and China also a restriction has been imposed on use of camera phones in schools and Government buildings.

Therefore, there is an urgent need to have a legislation on the regulation of use of camera phones in the country.

Hence this Bill.

VIJAY J. DARDA
MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 17 of the Bill empowers the Central Government to make rules for carrying out the purposes of the Bill. As the matter will relate to details only, the delegation of powers is of normal character.
RAJYA SABHA

A BILL
to provide for a code of conduct for users of mobile camera phones at certain places including public places; to regulate their use by children; to assign responsibilities on the user to respect the privacy of others and matters connected therewith or incidental thereto.

(Shri Vijay J. Darda, M.P)

MGIPM/MS—4151RS(55)—8-12-2006.
Home Office

Surveillance Camera Code of Practice

June 2013
Surveillance Camera Code of Practice

Presented to Parliament Pursuant to Section 30 (1) (a) of the Protection of Freedoms Act 2012

June 2013

London: The Stationery Office

£8.75
1. Introduction

2. Overview and Guiding Principles

3. The development or use of surveillance camera systems

4. The use or processing of images or other information obtained by virtue of such systems

5. Surveillance Camera Commissioner
Chapter 1: Introduction

Definitions

1.1 In this code:

- "Overt surveillance" means any use of surveillance for which authority does not fall under the 2000 Act.
- "Public place" has the meaning given by Section 16(b) of the Public Order Act 1986 and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.
- "Relevant authority" has the meaning given by Section 33(5) of the 2012 Act.
- "Surveillance camera systems" has the meaning given by Section 29(6) of the 2012 Act and is taken to include: (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c)\(^1\).
- "System Operator" - person or persons that take a decision to deploy a surveillance camera system, and/or are responsible for defining its purpose, and/or are responsible for the control of the use or processing of images or other information obtained by virtue of such system.
- "System User" - person or persons who may be employed or contracted by the system operator who have access to live or recorded images or other information obtained by virtue of such system.

Background

1.2 This code of practice is issued by the Secretary of State under Section 30 of the 2012 Act. It provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities (as defined by section 33 of the 2012 Act) in England and Wales who must have regard to the code when exercising any functions to which the code relates. Other operators and users of surveillance camera systems in England and Wales are encouraged to adopt the code voluntarily. It is a significant step in the ongoing process of delivering the government’s commitment to the “further regulation of CCTV” which it believes is a task that is best managed in gradual and incremental stages. As understanding and application of the code increases the government may consider including other bodies as relevant authorities who will have to have regard to the code.

---

\(^1\) Excludes any camera system with relevant type approval of a prescribed device under Section 20 of the Road Traffic Offenders Act 1988 used exclusively for enforcement purposes, which captures and retains an image only when the relevant offence is detected and with no capability to be used for any surveillance purpose. For example, for the enforcement of speeding offences.

\(^4\) Surveillance Camera Code of Practice pursuant to the Protection of Freedoms Act 2012
Purpose of the code

1.3 Surveillance camera systems are deployed extensively within England and Wales, and these systems form part of a complex landscape of ownership and operation. Where used appropriately, these systems are valuable tools which contribute to public safety and security and in protecting both people and property.

1.4 The government is fully supportive of the use of overt surveillance cameras in a public place whenever that use is: in pursuit of a legitimate aim; necessary to meet a pressing need; proportionate; effective, and; compliant with any relevant legal obligations.

1.5 The purpose of the code will be to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them. The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterised as surveillance by consent, and such consent on the part of the community must be informed consent and not assumed by a system operator. Surveillance by consent should be regarded as analogous to policing by consent. In the British model of policing, police officers are citizens in uniform. They exercise their powers to police their fellow citizens with the implicit consent of their fellow citizens. Policing by consent is the phrase used to describe this. It denotes that the legitimacy of policing in the eyes of the public is based upon a general consensus of support that follows from transparency about their powers, demonstrating integrity in exercising those powers and their accountability for doing so.

1.6 In order to achieve this, the code sets out guiding principles that should apply to all surveillance camera systems in public places. These guiding principles are designed to provide a framework for operators and users of surveillance camera systems so that there is proportionality and transparency in their use of surveillance, and systems are capable of providing good quality images and other information which are fit for purpose.

1.7 To support the practical application of these guiding principles by a system operator, the Surveillance Camera Commissioner will provide information and advice on appropriate and approved operational and technical standards for various aspects of surveillance camera systems and on appropriate and approved occupational and competency standards for persons using these systems or processing images and information obtained by these systems to supplement this code.

1.8 This code has been developed to address concerns over the potential for abuse or misuse of surveillance by the state in public places, with the activities of local authorities and the police the initial focus of regulation. However, the government fully recognises that many surveillance camera systems within public places are operated by the private sector, by the third sector or by other public authorities (for example, shops and shopping centres, sports grounds and other sports venues, schools, transport systems and hospitals). Informed by advice from the Surveillance Camera Commissioner, the government will keep the code under review and may in due course consider adding others to the list of relevant authorities pursuant to section 33(5)(k) of the 2012 Act.

---

2 A public authority will be bound by the Human Rights Act 1998 and will therefore be required to demonstrate a pressing need when undertaking surveillance as this may interfere with the qualified right to respect for private and family life provided under Article 8 of the European Charter of Human Rights. This is the case whether or not that public authority is a relevant authority. A system operator who is not a public authority should nevertheless satisfy themselves that any surveillance is necessary and proportionate.
Scope of surveillance activity to which this code applies

1.9 The code applies to the use of surveillance camera systems as defined in paragraph 1.1 that operate in public places in England and Wales, regardless of whether or not there is any live viewing, or recording of images or information or associated data.

1.10 Covert surveillance by public authorities (as defined in Part II of the 2000 Act) is not covered by this code but is regulated by the 2000 Act. Covert surveillance in public places by those who do not fall within the 2000 Act (for example, the private operator of a surveillance camera system in a shopping centre) may be used as part of a specific investigation in exceptional and justifiable circumstances. Any such covert use of private systems by or on behalf of a public authority (with the authority’s knowledge) immediately places such use within the bounds of the 2000 Act.

Effect of the Code

1.11 A relevant authority must follow a duty to have regard to the guidance in this code when, in exercising any of its functions, it considers that the future deployment or continued deployment of surveillance camera systems to observe public places may be appropriate. This can include the operation or use of any surveillance camera systems, or the use or processing of images or other information obtained by virtue of such systems. The duty to have regard to this code also applies when a relevant authority uses a third party to discharge relevant functions covered by this code and where it enters into partnership arrangements. Contractual provisions agreed after this code comes into effect with such third party service providers or partners must ensure that contractors are obliged by the terms of the contract to have regard to the code when exercising functions to which the code relates. The duty to have regard does not extend to such third party service providers or partners unless they themselves are a relevant authority.

1.12 When a relevant authority in England has civil parking enforcement functions under the Traffic Management Act 2004 or bus lane enforcement functions under the Transport Act 2000, and considers the use of surveillance camera systems in exercising those functions, it must have regard to the guidance in this code. The primary purpose of any surveillance camera system used as part of civil enforcement arrangements must be the safe and efficient operation of the road network by deterring motorists from contravening parking or road traffic restrictions. Motorists may regard enforcement by cameras as over-zealous and relevant authorities should use them sparingly. Such systems should, therefore, only be deployed where other means of enforcement are not practical and their effectiveness in achieving this purpose is subject to regular review. Where there is any conflict between this code and the secondary legislation made under the Traffic Management Act 2004 or the Transport Act 2000 relevant to those functions or the statutory guidance issued under section 87 of the Traffic Management Act 2004, the provisions made in or under the Traffic Management Act 2004 and the Transport Act 2000 shall apply.

1.13 When a relevant authority in England has civil enforcement functions for moving traffic contraventions under the London Local Authorities Act 1996 Part 2, the London Local Authorities Act 2000 Schedule 2 and the London Local Authorities and Transport for London Act 2003 Part 2, and considers the use of surveillance camera systems in exercising those functions, it must have regard to the guidance in this code. The primary purpose of any surveillance camera system used as part of civil enforcement arrangements must be the safe and efficient operation of the road network by deterring
motorists from contravening parking or road traffic restrictions. Motorists may regard enforcement by cameras as over-zealous and relevant authorities should use them sparingly. Such systems should, therefore, only be deployed where other means of enforcement are not practical and their effectiveness in achieving this purpose is subject to regular review. Where there is any conflict between this code and London Local Authorities Act 1996 Part 2, the London Local Authorities Act 2000 Schedule 2 and the London Local Authorities and Transport for London Act 2003 Part 2 relevant to those functions then that legislation shall apply.

1.14 When a relevant authority in Wales has civil parking, bus lane or moving traffic enforcement functions under the Traffic Management Act 2004 and considers the use of surveillance camera systems in exercising those functions, it must have regard to the guidance in this code. The primary purpose of any surveillance camera system used as part of civil enforcement arrangements must be the safe and efficient operation of the road network by deterring motorists from contravening parking or road traffic restrictions. Motorists may regard enforcement by cameras as over-zealous and relevant authorities should use them sparingly. Such systems should, therefore, only be deployed where other means of enforcement are not practical and their effectiveness in achieving this purpose is subject to regular review. Where there is any conflict between this code and the secondary legislation made under the Traffic Management Act 2004 relevant to those functions or the Statutory Guidance documents issued by the Welsh Government under section 87 of the Traffic Management Act 2004, then that legislation and guidance shall apply.

1.15 When a relevant authority has licensing functions and considers the use of surveillance camera systems as part of the conditions attached to a licence or certificate, it must in particular have regard to guiding principle one in this code. Any proposed imposition of a blanket requirement to attach surveillance camera conditions as part of the conditions attached to a licence or certificate is likely to give rise to concerns about the proportionality of such an approach and will require an appropriately strong justification and must be kept under regular review. Applications in relation to licensed premises must take into account the circumstances surrounding that application and whether a requirement to have a surveillance camera system is appropriate in that particular case. For example, it is unlikely that a trouble-free community pub would present a pressing need such that a surveillance camera condition would be justified. In such circumstances where a licence or certificate is granted subject to surveillance camera system conditions, the consideration of all other guiding principles in this code is a matter for the licensee as the system operator.

1.16 A failure on the part of any person to act in accordance with any provision of this code does not of itself make that person liable to criminal or civil proceedings. This code is, however, admissible in evidence in criminal or civil proceedings, and a court or tribunal may take into account a failure by a relevant authority to have regard to the code in determining a question in any such proceedings.

1.17 Other operators of surveillance camera systems who are not defined as relevant authorities are encouraged to adopt this code and its guiding principles voluntarily and make a public commitment to doing so. Such system operators are not, however, bound by any duty to have regard to this code.
Relevant documents

1.18 The Information Commissioner’s CCTV Code of Practice provides good practice guidance for those involved in operating CCTV and other surveillance camera systems which view or record images of individuals including information derived from those images that may be related to them such as a vehicle registration mark. Its primary purpose is to help those involved in such activities to comply with their legal obligations under the 1998 Act.

1.19 The covert surveillance and property interference code of practice published by the Home Office provides statutory guidance on the use of covert surveillance by public authorities under the 2000 Act. Further guidance on the application of the 2000 Act is available from the Office of the Surveillance Commissioners.

1.20 This code provides guidance on the use of surveillance camera systems but does not replace or remove any statutory obligations on operators or users of such systems to comply with the provisions of both the 1998 Act and the 2000 Act.
Chapter 2: Overview and Guiding Principles

2.1 Modern and forever advancing surveillance camera technology provides increasing potential for the gathering and use of images and associated information. These advances vastly increase the ability and capacity to capture, store, share and analyse images and information. This technology can be a valuable tool in the management of public safety and security, in the protection of people and property, in the prevention and investigation of crime, and in bringing crimes to justice. Technological advances can also provide greater opportunity to safeguard privacy. Used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need.

2.2 In general, any increase in the capability of surveillance camera system technology also has the potential to increase the likelihood of intrusion into an individual's privacy. The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, whilst others are qualified, meaning that it is permissible for the state to interfere with the right provided that the interference is in pursuit of a legitimate aim and the interference is proportionate. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR.

2.3 That is not to say that all surveillance camera systems use technology which has a high potential to intrude on the right to respect for private and family life. Yet this code must regulate that potential, now and in the future. In considering the potential to interfere with the right to privacy, it is important to take account of the fact that expectations of privacy are both varying and subjective. In general terms, one of the variables is situational, and in a public place there is a zone of interaction with others which may fall within the scope of private life. An individual can expect to be the subject of surveillance in a public place as CCTV, for example, is a familiar feature in places that the public frequent. An individual can, however, rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place.

---

3 Article 8 of the European Charter on Human Rights reads as follows:

Right to respect for private and family life

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 with the exercise of this right except such as is in accordance with the 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 prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
2.4 The decision to use any surveillance camera technology must, therefore, be consistent with a legitimate aim and a pressing need. Such a legitimate aim and pressing need must be articulated clearly and documented as the stated purpose for any deployment. The technical design solution for such a deployment should be proportionate to the stated purpose rather than driven by the availability of funding or technological innovation. Decisions over the most appropriate technology should always take into account its potential to meet the stated purpose without unnecessary interference with the right to privacy and family life. Furthermore, any deployment should not continue for longer than necessary.

2.5 The starting point for a system operator in achieving the most appropriate balance between public protection and individual privacy and thereby achieving overt surveillance by consent is to adopt a single set of guiding principles that are applicable to all surveillance camera systems in public places. Following these guiding principles allows a system operator to establish a clear rationale for any overt surveillance camera deployment in public places, to run any such system effectively, helps ensure compliance with other legal duties and to maximise the likelihood of achieving surveillance by consent.

Guiding Principles

2.6 System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.
Chapter 3: The development or use of surveillance camera systems

This chapter expands on guiding principles 1-4 which address the development or use of surveillance camera systems.

Principle 1 - Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

3.1.1 Surveillance camera systems operating in public places must always have a clearly defined purpose or purposes in pursuit of a legitimate aim and necessary to address a pressing need (or needs). Such a legitimate aim and pressing need might include national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. That purpose (or purposes) should be capable of translation into clearly articulated objectives against which the ongoing requirement for operation or use of the systems and any images or other information obtained can be assessed.

3.1.2 In assessing whether a system will meet its objectives, and in designing the appropriate technological solution to do so, a system operator should always consider the requirements of the end user of the images, particularly where the objective can be characterised as the prevention, detection and investigation of crime and the end user is likely to the police and the criminal justice system.

3.1.3 A surveillance camera system should only be used in a public place for the specific purpose or purposes it was established to address. It should not be used for other purposes that would not have justified its establishment in the first place. Any proposed extension to the purposes for which a system was established and images and information are collected should be subject to consultation before any decision is taken.

Principle 2 - The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3.2.1 The right to respect for private and family life set out in Article 8 of the ECHR enshrines in law a long held freedom enjoyed in England and Wales. People do, however, have varying and subjective expectations of privacy with one of the variables being situational. Deploying surveillance camera systems in public places where there is a particularly high expectation of privacy, such as toilets or changing rooms, should only be done to address a particularly serious problem that cannot be addressed by less intrusive means. Such deployment should be subject to regular review, at least annually, to ensure it remains necessary.
3.2.2 Any proposed deployment that includes audio recording in a public place is likely to require a strong justification of necessity to establish its proportionality. There is a strong presumption that a surveillance camera system must not be used to record conversations as this is highly intrusive and unlikely to be justified.

3.2.3 Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated. It should always involve human intervention before decisions are taken that affect an individual adversely.

3.2.4 This principle points to the need for a privacy impact assessment process to be undertaken whenever the development or review of a surveillance camera system is being considered to ensure that the purpose of the system is and remains justifiable, there is consultation with those most likely to be affected, and the impact on their privacy is assessed and any appropriate safeguards can be put in place. Where such an assessment follows a formal and documented process, such processes help to ensure that sound decisions are reached on implementation and on any necessary measures to safeguard against disproportionate interference with privacy. In the case of a public authority, this also demonstrates that both the necessity and extent of any interference with Article 8 rights has been considered.

3.2.5 A privacy impact assessment also helps assure compliance with obligations under the 1998 Act. Comprehensive guidance on undertaking a privacy impact assessment is available from the Information Commissioner's Office. This encourages organisations to devise and implement an assessment process that is appropriate and proportionate to their circumstances.

Principle 3 - There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

3.3.1 People in public places should normally be made aware whenever they are being monitored by a surveillance camera system, who is undertaking the activity and the purpose for which that information is to be used. This is an integral part of overt surveillance and is already a legal obligation under the 1998 Act. Furthermore, such awareness on the part of the public supports and informs the concept of surveillance by consent.

3.3.2 Surveillance by consent is dependent upon transparency and accountability on the part of a system operator. The provision of information is the first step in transparency, and is also a key mechanism of accountability. In the development or review of any surveillance camera system, proportionate consultation and engagement with the public and partners (including the police) will be an important part of assessing whether there is a legitimate aim and a pressing need, and whether the system itself is a proportionate response. Such consultation and engagement also provides an opportunity to identify any concerns and modify the proposition to strike the most appropriate balance between public protection and individual privacy.

---

4 The Surveillance Camera Commissioner will be a source of advice on validation of such systems.
3.3.3. This means ensuring effective engagement with representatives of those affected and in particular where the measure may have a disproportionate impact on a particular community. It is important that consultation is meaningful and undertaken at a stage when there is a realistic prospect of influencing developments.

3.3.4 System operators should be proactive in the provision of regularly published information about the purpose, operation and effect of a system. This is consistent with the government’s commitment to greater transparency on the part of public bodies.

3.3.5 In addition to the proactive publication of information about the stated purpose of a surveillance camera system, good practice includes considering the publication of information on the procedures and safeguards in place, impact assessments undertaken, performance statistics and other management information and any reviews or audits undertaken. Public authorities should consider including this information as part of their publication schemes under the Freedom of Information Act 2000.

3.3.6 This is not to imply that the exact location of surveillance cameras should always be disclosed if to do so would be contrary to the interests of law enforcement or national security.

3.3.7 A system operator should have an effective procedure for handling concerns and complaints from individuals and organisations about the use of surveillance camera systems. Information about complaints procedures should be made readily available to the public. Where a complaint is made and the complainant not satisfied with the response there should be an internal review mechanism in place using a person not involved in handling the initial complaint. Complaints must be handled in a timely fashion and complainants given an indication of how long a complaint may take to handle at the outset.

3.3.8 Once a complaint has been concluded information should be provided to the complainant about any regulatory bodies who may have jurisdiction in that case such as the Information Commissioner or the Investigatory Powers Tribunal.

3.3.9 Where a complaint or other information comes to the attention of a relevant authority or other system operator that indicates criminal offences may have been committed in relation to a surveillance camera system then these matters should be referred to the appropriate body, such as the police or the Information Commissioner for any offences under the 1998 Act.

3.3.10 In line with government commitment towards greater transparency on the part of public authorities a system operator should publish statistical information about the number and nature of complaints received and how these have been resolved on an annual basis at least.

3.3.11 The government’s further commitment to ‘open data’ means that public authorities should consider making information available in reusable form so others can develop services based on this data. This would extend to information about surveillance camera systems.

3.3.12 The Surveillance Camera Commissioner has no statutory role in relation to the investigation and resolution of complaints. System operators should, however, be prepared to share information about the nature of complaints with the Surveillance Camera Commissioner on an ad hoc and where appropriate anonymised basis to assist in any review of the operation of this code of practice.
Principle 4 - There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

3.4.1 Persons considering the need to develop a surveillance camera system should give due consideration to the establishment of proper governance arrangements. There must be clear responsibility and accountability for such a system. It is good practice to have a designated individual responsible for the development and operation of a surveillance camera system, for ensuring there is appropriate consultation and transparency over its purpose, deployment and for reviewing how effectively it meets its purpose.

3.4.2 Where a system is jointly owned or jointly operated, the governance and accountability arrangements should be agreed between the partners and documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and procedures for the resolution of any differences between the parties or changes of circumstance.

3.4.3 A surveillance camera system may be used for more than one purpose. For example, one purpose might be crime prevention and detection, and another traffic management. Accountability for each purpose may rest within different elements of a system operator’s management structure. Should that be the case, then it is good practice for the governance arrangements to include those accountable for each purpose and facilitate effective joint working, review and audit, decision making and public engagement.
Chapter 4: The use or processing of images or other information obtained by virtue of such systems

This chapter expands on guiding principles 5-12 which address the use or processing of images and information.

Principle 5 - Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

4.5.1 There are significant benefits in having clear policies and procedures for the operation of any surveillance. This can not only aid the effective management and use of a surveillance camera system but also help ensure that any legal obligations affecting the use of such a system are addressed.

4.5.2 A surveillance camera system operator is encouraged to follow a quality management system as a major step forward in controlling and improving their key processes. Where this is done through certification against a quality management standard it can provide a robust operating environment with the additional benefit of reassurance for the public that the system is operated responsibly and effectively, and the likelihood of any breach of individual privacy is greatly reduced.

4.5.3 It is good practice that the communication of rules, policies and procedures should be done as part of the induction and ongoing professional training and development of all system users. This should maximise the likelihood of compliance by ensuring system users are competent, have relevant skills and training on the operational, technical and privacy considerations and fully understand the policies and procedures. It is requirement of the 1998 Act that organisations ensure the reliability of staff having access to personal data, including images and information obtained by surveillance camera systems.

4.5.4 Wherever there are occupational standards available which are relevant to the roles and responsibilities of their system users, a systems operator should consider the benefits and any statutory requirements associated with such occupational standards.

4.5.5 The Surveillance Camera Commissioner will provide advice and guidance on relevant quality management and occupational competency standards.

4.5.6 Wherever a surveillance camera system covers public space a system operator should be aware of the statutory licensing requirements of the Private Security Industry Act 2001. Under these requirements, the Security Industry Authority (SIA) is charged with licensing individuals working in specific sectors of the private security industry. A public space surveillance (CCTV) licence is required when operatives are supplied under a contract for services. It is a criminal offence for staff to carry out licensable activities without an SIA licence.
4.5.7 SIA licensing is dependent upon evidence that an individual is fit and proper to fulfil the role, and evidence of their ability to fulfil a role effectively and safely with the right skills and knowledge. There are various relevant qualifications available, and training to attain these is delivered by a range of different accredited providers.

4.5.8 Even where there is no statutory licensing requirement, it is good practice for a system operator to ensure that all staff who either manage or use a surveillance camera system, or use or process the images and information obtained by virtue of such systems have the necessary skills and knowledge.

Principle 6 - No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

4.6.1 Images and information obtained from a surveillance camera system should not be kept for longer than necessary to fulfil the purpose for which they were obtained in the first place. This period should be decided in advance and be the minimum period necessary. This is also a requirement of the 1998 Act and further guidance on this is contained in the ICO CCTV code of practice.

4.6.2 The retention period for different surveillance camera systems will vary due to the purpose for the system and how long images and other information need to be retained so as to serve its intended purpose. It is not, therefore, possible to be prescriptive about maximum or minimum periods. Initial retention periods should be reviewed by a system operator and reset in the light of experience. A proportionate approach should always be used to inform retention periods and these should not be based upon infrequent exceptional cases.

4.6.3 Although images and other information should not be kept for longer than necessary to meet the purposes for recording them, on occasions, a system operator may need to retain images for a longer period, for example where a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation.

Principle 7 - Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

4.7.1 The disclosure of images and other information obtained from a surveillance camera system must be controlled and consistent with the stated purpose for which the system was established. Disclosure of images or information may be appropriate where the 1998 Act makes exemptions which allow it provided that the applicable requirements of the 1998 Act are met, or where permitted by other legislation such as the Counter Terrorism Act 2008. These exemptions include where non-disclosure would be likely to prejudice the prevention and detection of crime, and for national security purposes. Where a system operator declines a request for disclosure from a law enforcement agency there is provision under Section 9 of and Schedule 1 to the Police and Criminal Evidence Act 1984 to seek a production order from a magistrate.
4.7.2 There may be other limited occasions when disclosure of images to another third party, such as a person whose property has been damaged, may be appropriate. Such requests for images or information should be approached with care and in accordance with the 1998 Act, as a wide disclosure may be an unfair intrusion into the privacy of the individuals concerned.

4.7.3 A system operator should have clear policies and guidelines in place to deal with any requests that are received. In particular:

- Arrangements should be in place to restrict disclosure of images in a way consistent with the purpose for establishing the system.
- Where images are disclosed consideration should be given to whether images of individuals need to be obscured to prevent unwarranted identification.
- Those that may handle requests for disclosure should have clear guidance on the circumstances in which disclosure is appropriate.
- The method of disclosing images should be secure to ensure they are only seen by the intended recipient.
- Appropriate records should be maintained.

4.7.4 Judgements about disclosure should be made by a system operator. They have discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. Once they have disclosed an image to another body, such as the police, then the recipient becomes responsible for their copy of that image. If the recipient is a relevant authority, it is then the recipient’s responsibility to have regard to this code of practice and to comply with any other legal obligations such as the 1998 Act and the Human Rights Act 1998 in relation to any further disclosures.

4.7.5 Individuals can request images and information about themselves through a subject access request under the 1998 Act. Detailed guidance on this and matters such as when to withhold images of third parties caught in images is included in the ICO CCTV code of practice.

4.7.6 Requests for information from public bodies may be made under the Freedom of Information Act 2000. Detailed guidance on these obligations is included in the ICO CCTV code of practice.

Principle 8 - Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

4.8.1 Approved standards may apply to the system functionality, the installation and the operation and maintenance of a surveillance camera system. These are usually focused on typical CCTV installations, however there may be additional standards applicable where the system has specific advanced capability such as ANPR, video analytics or facial recognition systems, or where there is a specific deployment scenario, for example the use of body-worn video recorders.
4.8.2 Approved standards are available to inform good practice for the operation of surveillance camera systems, including those developed domestically by the British Standards Institute, at a European level by the Comité Européen de Normalisation Electrotechnique\(^5\), or at a global level by the International Electrotechnical Commission. A system operator should consider any approved standards which appear relevant to the effective application of technology to meet the purpose of their system, and taking steps to secure certification against those standards.

4.8.3 Such certification is likely to involve assessment by an independent certification body. This has benefits for a system operator in that the effectiveness of a system is likely to be assured and in demonstrating to the public that suitable standards are in place and being followed.

4.8.4 A current list of recommended standards for consideration by a system operator will be maintained and made available by the Surveillance Camera Commissioner. Such a list will provide detailed guidance on suitable standards and the bodies that are able to accredit performance against such standards.

**Principle 9** Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

4.9.1 Putting effective security safeguards in place helps ensure the integrity of images and information should they be necessary for use as evidence in legal proceedings. This also helps to foster public confidence in system operators and how they approach the handling of images and information.

4.9.2 Under the 1998 Act, those operating surveillance camera systems or who use or process images and information obtained by such systems must have a clearly defined policy to control how images and information are stored and who has access to them. The use or processing of images and information should be consistent with the purpose for deployment, and images should only be used for the stated purpose for which collected.

4.9.3 Security extends to technical, organisational and physical security and there need to be measures in place to ensure that this is the case and guard against unauthorised use, access or disclosure. The ICO CCTV code of practice gives helpful guidance on achieving this in practice.

**Principle 10** - There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

4.10.1 Good practice dictates that a system operator should review the continued use of a surveillance camera system on a regular basis, at least annually, to ensure it remains necessary, proportionate and effective in meeting its stated purpose for deployment.

4.10.2 As part of the regular review of the proportionality and effectiveness of a surveillance camera system a system operator should assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.

\(^5\) CENELEC is also known as the European Committee for Electrotechnical Standardization
4.10.3 In reviewing the continued use of a surveillance camera system a system operator should consider undertaking an evaluation to enable comparison with alternative interventions with less risk of invading individual privacy, and different models of operation (to establish for example any requirement for 24 hour monitoring). In doing so, there should be consideration of an assessment of the future resource requirements for meeting running costs, including staffing, maintenance and repair.

4.10.4 A system operator should make a summary of such a review available publicly as part of the transparency and accountability for the use and consequences of its operation.

Principle 11 - When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

4.11.1 The effectiveness of a surveillance camera system will be dependent upon its capability to capture, process, analyse and store images and information at a quality which is suitable for its intended purpose. Wherever the purpose of a system includes crime prevention, detection and investigation, it should be capable through processes, procedures and training of system users, of delivering images and information that is of evidential value to the criminal justice system. Otherwise, the end user of the images, who are likely to be the police and the criminal justice system, will not be able to play their part effectively in meeting the intended purpose of the system.

4.11.2 It is important that there are effective safeguards in place to ensure the forensic integrity of recorded images and information and its usefulness for the purpose for which it is intended to be used. Recorded material should be stored in a way that maintains the integrity of the image and information, with particular importance attached to ensuring that meta data (e.g. time, date and location) is recorded reliably, and compression of data does not reduce its quality. This is to ensure that the rights of individuals recorded by a surveillance camera system are protected and that the material can be used as evidence in court. To do this the medium on which the images and information are stored will be important, and access must be restricted. A record should be kept as an audit trail of how images and information are handled if they are likely to be used as exhibits for the purpose of criminal proceedings in court. Once there is no longer a clearly justifiable reason to retain the recorded images and information, they should be deleted.

4.11.3 It is important that digital images and other related information can similarly be shared with ease with appropriate law enforcement agencies if this is envisaged when establishing a system. If this interoperability cannot be readily achieved it may undermine the purpose for deploying the system.

4.11.4 It is therefore essential that any digital images and information likely to be shared with law enforcement agencies and the criminal justice system are in a data format that is interoperable and can be readily exported, and then stored and analysed without any loss of forensic integrity. In particular:
• A system user should be able to export images and information from a surveillance camera system when requested by a law enforcement agency.
• The export of images and information should be possible without interrupting the operation of the system.
• The exported images and information should be in a format which is interoperable and can be readily accessed and replayed by a law enforcement agency.
• The exported images and information must preserve the quality of the original recording and any associated meta data (e.g. time, date and location).

Principle 12 - Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

4.12.1 Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose.

4.12.2 A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on the reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database.

4.12.3 There may be occasions when the inclusion of information about an individual in a reference database with the intention of undertaking surveillance can be considered as covert surveillance and thus fall with the bounds of the 2000 Act. Further guidance on the application of the 2000 Act is available in the Home Office statutory covert surveillance and property interference code of practice and from the Office of the Surveillance Commissioners.
5.1 The Surveillance Camera Commissioner, (the commissioner), is a statutory appointment made by the Home Secretary under Section 34 of the 2012 Act. The commissioner’s statutory functions are:

a) encouraging compliance with this code;
b) reviewing the operation of this code; and
c) providing advice about this code (including changes to it or breaches of it).

5.2 In order to fulfil these functions effectively, the commissioner must work closely with other regulators including the Information Commissioner and the Chief Surveillance Commissioner. It is for the commissioner and other regulators to determine how best to maintain and formalise these relationships, to agree gateways through which issues flow between the public and the commissioners and how best to publicise and report on arrangements to support these relationships which will be critical in ensuring the success of the code in meeting its purpose.

Ways of working

5.3 The commissioner has no enforcement or inspection powers. In encouraging compliance with the code he should consider how best to ensure that relevant authorities are aware of their duty to have regard for the code and how best to encourage its voluntary adoption by other operators of surveillance camera systems.

5.4 The commissioner is expected to provide advice about the relevant operational, technical, quality management and occupational competency standards which are available for a system operator. A system operator can then consider these standards in determining how best to meet the purpose of their surveillance camera system whilst meeting legal obligations, making effective use of it, and safeguarding privacy considerations. Such advice can be updated to reflect developments in both the available technology and professional practice.

5.5 In reviewing the operation of the code, the commissioner should consider the impact of this system of regulation against published success criteria and the opportunities to improve compliance in line with better regulation principles.

5.6 The commissioner should provide advice and information to the public and system operators about the effective, appropriate, proportionate and transparent use of surveillance camera systems and should consider how best to make that information available. Such advice should complement the content of this code, and may for example provide additional detail on good practice, advice on the effectiveness of surveillance cameras and how this might be assessed, or on the proportionate application of any new technological developments in surveillance camera systems. Such advice could, for example, include the preparation of a manual of regulation that sets out how the commissioner will fulfill his functions.
5.7 The commissioner may establish a non-statutory advisory council with specialist sub-groups to support him in fulfilling his functions. Any advisory council or specialist sub-group must have representation from such persons appearing to the commissioner to be representative of the views of relevant authorities and from the Home Office.

5.8 The commissioner must prepare a report about the exercise of his functions during the reporting period, and:

a) give a copy of the report to the Secretary of State;
b) the Secretary of State must lay a copy of the report before Parliament; and
c) the commissioner must publish the report.

5.9 The reporting periods are set out in Section 35 of the 2012 Act.
CHAPTER I
PRELIMINARY

1. Short title, extent and commencement.
2. Definitions.
3. Principles applicable to protecting privacy.

CHAPTER II
RIGHT TO PRIVACY

4. Right to privacy.
5. Exemptions.

CHAPTER III
PROTECTION OF PERSONAL DATA

6. Collection of personal data.
7. Storage and destruction of personal data.
8. Processing of personal data.
10. Disclosure of personal data.
11. Quality and accuracy of personal data.
12. Special provisions for sensitive personal data.
13. Special provisions for intelligence organisations.

CHAPTER IV
INTERCEPTION OF COMMUNICATIONS

14. Bar against interception of communications.
15. Prior authorisation by the Chief Privacy Commissioner.
16. Authorisation by Home Secretary in emergent circumstances.
17. Duration of interception.
18. Duty to inform the person concerned.

CHAPTER V
SURVEILLANCE
22. Bar against surveillance.
23. Surveillance by the State.
24. Surveillance by private persons or entities.
25. Duration of surveillance.
26. Duty to inform the person concerned.
27. Security and duty of confidentiality and secrecy.
29. Storage of surveillance.

CHAPTER VI
THE PRIVACY COMMISSION

31. Term of office, conditions of service, etc. of Chief Privacy Commissioner and Privacy Commissioners.
32. Removal of Chief Privacy Commissioner and Privacy Commissioners from office in certain circumstances.
33. Functions of the Privacy Commission.
34. Secretary, officers and other employees of the Privacy Commission.
35. Salaries, etc. be defrayed out of the Consolidated Fund of India.
36. Vacancies, etc. not to invalidate proceedings of the Privacy Commission.
37. Chief Privacy Commissioner, Privacy Commissioners and employees of the Privacy Commission to be public servants.
38. Location of the office of the Privacy Commission.
39. Procedure to be followed by the Privacy Commission.
40. Power relating to inquiries.
41. Decisions of the Privacy Commission.
42. Proceedings before the Privacy Commission to be judicial proceedings.

CHAPTER VII
OFFENCES AND PENALTIES

43. Punishment for offences related to personal data.
44. Punishment for offences related to interception of communication.
45. Punishment for offences related to surveillance.
46. Abetment and repeat offenders.
47. Offences by companies.
48. Cognisance.
49. General penalty.
50. Punishment to be without prejudice to any other action.

CHAPTER VIII
MISCELLANEOUS

51. Power to make rules.
52. Bar of jurisdiction.
53. Protection of action taken in good faith.
54. Power to remove difficulties.
55. Act to have overriding effect.
THE PRIVACY (PROTECTION) BILL, 2013

A BILL
to establish an effective regime to protect the privacy of all persons and their personal data from Governments, public authorities, private entities and others, to set out conditions upon which surveillance of persons and interception and monitoring of communications may be conducted, to constitute a Privacy Commission, and for matters connected therewith and incidental thereto.

WHEREAS the right to privacy is an inalienable right of all persons;

AND WHEREAS the delivery of goods and services often requires personal data from persons and this personal data is processed, stored and transmitted across international borders without the informed consent of the persons to whom it pertains;

AND WHEREAS democracy requires interceptions of communications and surveillance to be conducted in a systematic and transparent manner subservient to the rule of law;

AND WHEREAS it is necessary to harmonise these conflicting interests while preserving the paramountcy of the democratic ideal;

NOW, THEREFORE, it is expedient to provide for an enforceable means to protect the privacy of persons.

BE IT ENACTED by Parliament in the Sixty-fourth Year of the Republic of India as follows –

CHAPTER I
Preliminary

1. Short title, extent and commencement. – (1) This Act may be called the Privacy (Protection) Act, 2013.
   
   (2) It extends to the whole of India.
   
   (3) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

2. Definitions. – In this Act and in any rules made thereunder, unless the context otherwise requires,

   (a) “anonymise” means, in relation to personal data, the removal of all data that may, whether directly or indirectly in conjunction with any other data, be used to identify a natural person;

   (b) “appropriate government” means, in relation to the Central Government or a Union Territory Administration, the Central Government; in relation a State Government, that State Government; and, in relation to a public authority which is established, constituted, owned, controlled or substantially financed by funds provided directly or indirectly –
(i) by the Central Government or a Union Territory Administration, the Central Government;
(ii) by a State Government, that State Government;

c) “armed force” means any body raised or constituted pursuant to or in connection with, or presently governed by, the Army Act, 1950 (46 of 1950), the Indian Reserve Forces Act, 1888 (4 of 1888), the Territorial Army Act, 1948 (6 of 1948), the Navy Act, 1957 (62 of 1957), the Air Force Act, 1950 (45 of 1950), the Reserve and Auxiliary Air Forces Act, 1952 (62 of 1952), the Coast Guard Act, 1978 (30 of 1978) or the Assam Rifles Act, 2006 (47 of 2006);

d) “authorised officer” means an officer, not below the rank of a Gazetted Officer, of an All India Service or a Central Civil Service, as the case may be, who is empowered by the Central Government, by notification in the Official Gazette, to intercept a communication of another person or carry out surveillance of another person under this Act;

e) “biometric data” means any data relating to the physical, physiological or behavioural characteristics of a person which allow their unique identification including, but not restricted to, facial images, finger prints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and speech recognition;

f) “Chief Privacy Commissioner” and “Privacy Commissioner” mean the Chief Privacy Commissioner and Privacy Commissioner appointed under sub-section (1) of section 30;

g) “collect”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a police force, armed force, intelligence organisation, public authority, company, person, State or other entity obtaining, or coming into the knowledge or possession of, any personal data of another person;

h) “communication” means a word or words, spoken, written or indicated, in any form, manner or language, encrypted or unencrypted, meaningful or otherwise, and includes visual representations of words, ideas, symbols and images, whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission;

i) “competent organisation” means an organisation or public authority listed in the Schedule;

j) “deoxyribonucleic acid data” means all data, of whatever type, concerning the characteristics of a person that are inherited or acquired during early prenatal development;

k) “destroy”, with its grammatical variations and cognate expressions, means, in relation to personal data, to cease the existence of, by deletion, erasure or otherwise, any personal data;

l) “disclose”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a person coming into the knowledge or possession of any personal data of another person;

m) “intelligence organisation” means an intelligence organisation under the Intelligence Organisations (Restriction of Rights) Act, 1985 (58 of 1985) and includes the National Investigation Agency constituted under sub-section (1) of section 3 of the National Investigation Agency Act, 2008 (34 of 2008);

n) “interception” or “intercept” means any activity intended to capture, read, listen to or understand the communication of a person;

(o) “officer-in-charge of a police station” shall have the meaning ascribed to it under clause (o) of section 2 of the Code of Criminal Procedure, 1973 (2 of 1974);
(p) "personal data" means any data which relates to a natural person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data;

(q) "police force" means –

(i) any body raised or constituted by the appropriate government for the preservation of law and order;
(ii) the bodies raised or constituted pursuant to or in connection with, or presently governed by, the Police Act, 1861 (5 of 1861), the Central Reserve Police Force Act, 1949 (66 of 1949), the Border Security Force Act, 1968 (47 of 1968), the Indo-Tibetan Border Police Force Act, 1992 (35 of 1992), the Sashastra Seema Bal Act, 2007 (53 of 2007), the Central Industrial Security Force Act, 1968 (50 of 1968), the Railway Protection Force Act, 1957 (23 of 1957) or the National Security Guard Act, 1986 (47 of 1986); and
(iii) any police forces raised or constituted by the States, armed or otherwise;

(r) “prescribed” means prescribed by rules made under this Act;
(s) “Privacy Commission” means the Privacy Commission constituted under sub-section (1) of section 30;
(t) “Privacy Officer” means the Privacy Officer designated under sub-section (3) of section 19, sub-section (3) of section 27 and sub-section (4) of section 17.
(u) “process”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or operation which is performed upon personal data, whether or not by automated means;
(v) “public authority” shall have the meaning ascribed to it under clause (h) of section 2 of the Right to Information Act, 2005 (22 of 2005);
(w) “receive”, with its grammatical variations and cognate expressions, means, in relation to personal data, to come into the knowledge or possession of any personal data of another person;
(x) “sensitive personal data” means personal data as to a person’s –

(i) biometric data; and
(ii) deoxyribonucleic acid data;

(y) “store”, with its grammatical variations and cognate expressions, means, in relation to personal data, to retain, in any form or manner and for any purpose or reason, any personal data of another person;
(z) “surveillance” means any activity intended to watch, monitor, record or collect, or to enhance the ability to watch, record or collect, any images, signals, data, movement, behaviour or actions, of a person, a group of persons, a place or an object, for the purpose of obtaining information of a person.

3. Principles applicable to protecting privacy. – In exercising the powers conferred by this Act, regard shall be had to the following considerations, namely –

(a) that personal data belongs solely to the person to whom it pertains;
(b) that personal data is required by governments and commercial service providers and others to enable public safety, good governance and the delivery of services without undue delay;
(c) that the right to privacy is recognised as a fundamental human right by various international treaties to which India is a party;
(d) that intrusions into privacy need always be measured by necessity and tempered by proportionality;
(e) that the right to privacy is essential to the maintenance of a democratic society;
(f) that the right to privacy cannot override the right to information;
(g) that privacy must be upheld by a competent authority that is independent, impartial, well resourced and free from unwarranted influence.

CHAPTER II
RIGHT TO PRIVACY

4. Right to privacy. – (1) Notwithstanding anything contained in any other law for time being in force but subject to the provisions of this Act, all persons shall have a right to privacy.

(2) For the purpose of sub-section (1), no person shall collect, store, process, disclose or otherwise handle any personal data of another person, intercept any communication of another person, or carry out surveillance of another person except in accordance with the provisions of this Act.

5. Exemptions. – Nothing in this Act shall apply to –

(a) the collection, storage or processing of personal data for personal or family use; or
(b) surveillance by a resident of his residential property or premises.

CHAPTER III
PROTECTION OF PERSONAL DATA

6. Collection of personal data. – (1) No person shall collect any personal data of another person that is not necessary for the achievement of a purpose that is connected to a stated function of the person seeking its collection.

(2) No person shall collect any personal data of another person without obtaining the prior consent of the person to whom it pertains and such consent may be obtained in any manner, and through any medium, but shall not be obtained as a result of a threat, duress or coercion.

(3) For the purpose of sub-section (2), a person seeking to collect any personal data of another person shall, prior to its collection, inform that person of the following details in respect of his personal data, namely: –

(a) when it will be collected;
(b) its content and nature;
(c) the purpose of its collection;
(d) the manner in which it will be used;
(e) the persons to whom it will be made available;
(f) the duration for which it will be stored;
(g) the manner in which it may be accessed, checked and modified;
(h) the security practices and other safeguards, if any, to which it will be subject;
(i) the privacy policies and other policies, if any, that will protect it;
(j) whether, and the conditions and procedure upon which, it may be disclosed to others;
(k) the time and manner in which it will be destroyed; and,
(l) the procedure for recourse in case of any grievance in relation to it.

(4) Personal data collected in respect of a grant of consent by the person to whom it pertains shall, if that consent is subsequently withdrawn for any reason, be destroyed forthwith:

Provided that the person who collected the personal data in respect of which consent is subsequently withdrawn may, only if the personal data is necessary for the delivery of any good or the provision of any service, not deliver that good or deny that service to the person who withdrew the grant of consent.

7. Storage and destruction of personal data. – (1) No person shall store any personal data of another person for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose is achieved or ceases to exist for any reason, for any period following such achievement or cessation.

(2) Save as provided in sub-section (3), any personal data collected or received in relation to the achievement of a purpose shall, if that purpose is achieved or ceases to exist for any reason, be destroyed forthwith.

(3) Notwithstanding anything contained in this section, any personal data may be stored for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if –

(a) the person to whom it pertains grants his consent to such storage prior to the purpose for which it was collected or received being achieved or ceasing to exist; or
(b) it is required to be stored for historical, statistical or research purposes under the provisions of an Act of Parliament:

Provided that only that amount of personal data that is necessary to achieve the purpose of storage under this sub-section shall be stored and any personal data that is not required to be stored for such purpose shall be destroyed forthwith:

Provided further that any personal data stored under this sub-section shall, to the extent possible, be anonymised.

8. Processing of personal data. – (1) No person shall process any personal data of another person that is not necessary for the achievement of the purpose for which it was collected or received.

(2) Save as provided in sub-section (3), no personal data shall be processed for any purpose other than the purpose for which it was collected or received.

(3) Notwithstanding anything contained in this section, any personal data may be processed for a purpose other than the purpose for which it was collected or received if the person to whom it pertains grants his consent to such processing and only that amount of personal data that is necessary to achieve the other purpose is processed.

9. Security of personal data and duty of confidentiality. – (1) No person shall collect, receive, store, process or otherwise handle any personal data of another person without implementing measures,
including, but not restricted to, technological, physical and administrative measures, adequate to secure its confidentiality, secrecy, sanctity and safety, including from theft, loss, damage or destruction.

(2) Any person who collects, receives, stores, processes or otherwise handles any personal data of another person shall be subject to a duty of confidentiality and secrecy in respect of it.

(3) Without prejudice to the provisions of this section, any person who collects, receives, stores, processes or otherwise handles any personal data of another person shall, if its confidentiality, secrecy, sanctity or safety is violated by theft, loss, damage or destruction, or as a result of any disclosure contrary to the provisions of this Act, or for any other reason whatsoever, as soon as he becomes aware of such violation, notify the person to whom it pertains, in such form and manner as may be prescribed, forthwith.

10. Disclosure of personal data. – (1) Save as provided in this section, no person shall disclose to any other person, or otherwise cause any other person to receive, the content or nature of any personal data, including any other details in respect thereof, except to the person to whom it pertains.

(2) No person shall disclose any personal data of another person without obtaining the prior consent of the person to whom it pertains and such consent may be obtained in any manner, and through any medium, but shall not be obtained as a result of a threat, duress or coercion.

(3) For the purpose of sub-section (2), a person seeking to disclose any personal data of another person shall, prior to its disclosure, inform that person of the following details in respect of his personal data, namely:

(a) when it will be disclosed;
(b) the persons to whom it will be disclosed;
(c) the purpose of its disclosure;
(d) the security practices and other safeguards, if any, to which it will be subject;
(e) the privacy policies and other policies, if any, that will protect it; and
(f) the procedure for recourse in case of any grievance in relation to it.

(4) Notwithstanding anything contained in this section, any person who collects, receives, stores, processes or otherwise handles any personal data may disclose it to a person other than the person to whom it pertains, whether located in India or otherwise, for the purpose only of processing it to achieve the purpose for which it was collected if such a disclosure is pursuant to an agreement that explicitly binds the person receiving it to same or stronger measures in respect of its storage, processing, destruction, disclosure or other handling as are contained in this Act.

(5) Notwithstanding anything contained in this section, if the disclosure of any personal data is necessary to –

(a) prevent a reasonable threat to national security, defence or public order, or
(b) prevent, investigate or prosecute a cognisable offence,

any person may, upon receiving an order in writing from an officer-in-charge of a police station, in such form and manner as may be prescribed, disclose the personal data that is the subject of the order without seeking the consent of the person to whom it pertains:

Provided that an order for the disclosure of personal data made under this sub-section shall not require the disclosure of any personal data that is not necessary to achieve the purpose for which the disclosure is sought:
Provided further that the person to whom any personal data disclosed under this sub-section pertains shall be notified, in such form and manner as may be prescribed, of the disclosure of his personal data, including details of its content and nature or any other details in respect thereof, and the identity of the person it was disclosed to, and any other details in respect thereof, forthwith.

11. Quality and accuracy of personal data. – (1) Any person who collects, receives, stores, processes or otherwise handles any personal data of another person shall, to the extent possible, ensure that it is not inaccurate or misleading and, where necessary, is kept up to date.
(2) No person who collects, receives, stores, processes or otherwise handles any personal data shall deny, to the person to whom any personal data so collected, received, stored, processed or otherwise handled pertains, the opportunity to review it and, where necessary, rectify anything that is inaccurate, misleading or not up to date.
(3) Without prejudice to the provisions of sub-section (4) of section 6, any person to whom any personal data collected, received, stored, processed or otherwise handled under this Act pertains may, if it is not necessary to achieve the purpose of its collection, reception, storage, processing or other handling, demand its destruction, and the person so collecting, receiving, storing, processing or otherwise handling that personal data shall destroy it forthwith.

12. Special provisions for sensitive personal data. – Notwithstanding anything contained in this Act and the provisions of any other law for the time being in force –
(a) no person shall store sensitive personal data for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation;
(b) no person shall process sensitive personal data for a purpose other than the purpose for which it was collected or received;
(c) no person shall disclose sensitive personal data to another person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any sensitive personal data, including any other details in respect thereof, except the person to whom it pertains.

13. Special provisions for intelligence organisations. – (1) Notwithstanding anything contained in this Act, the provisions of section 6, section 7, section 8, sub-section (4) of section 10 and section 11 shall not apply in respect of an intelligence organisation.
(2) Any intelligence organisation seeking to collect any personal data of another person shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.
(3) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, if he is satisfied that the collection of the personal data is necessary –
(a) to prevent a reasonable threat to national security, defence or public order, or
(b) to prevent, investigate or prosecute a cognisable offence,
for reasons to be recorded in writing, order the collection of the personal data.
(4) Notwithstanding anything contained in sub-section (2) and sub-section (3), if the Central Government is satisfied that a grave threat to national security, defence or public order exists, it may, for reasons to be recorded in writing, order the collection of any personal data.

(5) Before the expiry of a period of seven days from the date of an order for collection of personal data made under sub-section (4), the intelligence organisation that collected the personal data shall notify the Chief Privacy Commissioner of the fact of such collection, the name and address of the person to whom the personal data pertains and shall furnish a copy of the order of the Central Government authorising the collection of the personal data.

(6) No intelligence organisation shall process or store any personal data of another person without implementing measures to secure that –

(a) the number of persons within that intelligence organisation to whom it is made available, and
(b) the extent to which it is copied,
is limited to the minimum that is necessary to fulfill the purpose for which it is processed or stored, as the case may be.

(7) Any intelligence organisation that processes or stores personal data of another person shall, before the expiry of a period of seven days from the date of the processing or storage, as the case may be, notify the Chief Privacy Commissioner of the fact of such processing or storage and the name and address of the person to whom the personal data pertains.

CHAPTER IV
INTERCEPTION OF COMMUNICATIONS

14. Bar against interception of communications. – (1) Notwithstanding anything contained in any other law for the time being in force, but save as provided in this chapter, no person shall intercept, or cause to be intercepted, any communication of another person save in pursuance of an order by the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(2) No interception of any communication shall be ordered or carried out that is not necessary to achieve the purpose for which the interception is sought.

15. Prior authorisation by the Chief Privacy Commissioner. – (1) Any authorised officer seeking to intercept any communication of another person shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(2) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, if he is satisfied that the interception is necessary –

(a) to prevent a reasonable threat to national security, defence or public order, or
(b) to prevent, investigate or prosecute a cognisable offence,

for reasons to be recorded in writing addressed to the authorised officer, order the interception of the communication.

(3) Prior to issuing an order for interception of any communication, the Chief Privacy Commissioner, or any other person authorised by him in this behalf, shall satisfy himself that all other
lawful means to acquire the information sought to be intercepted have been exhausted and that the proposed interception is reasonable, proportionate and not excessive.

(4) Any interception of any communication ordered, authorised or carried out prior to the commencement of this Act shall, immediately upon the constitution of the Privacy Commission, be reported to the Chief Privacy Commissioner.

16. Authorisation by Home Secretary in emergent circumstances. – (1) Notwithstanding anything contained in section 15, if the Home Secretary of the appropriate government is satisfied that a grave threat to national security, defence or public order exists, he may, for reasons to be recorded in writing, order the interception of any communication.

(2) No order for interception of any communication made under this section shall be valid upon the expiry of a period of seven days from the date of the order.

(3) Before the expiry of a period of seven days from the date of an order for interception made under this section, the person who carried out the interception of communication shall notify the Chief Privacy Commissioner of the fact of such interception, the name and address of the person whose communication is being intercepted, and the duration of the interception and, furthermore, shall furnish a copy of the order of the Home Secretary authorising the interception.

17. Duration of interception. – (1) An order for interception of any communication shall specify the period of its validity and, upon the expiry of the validity of the order, all interception carried out in relation to that order shall cease forthwith:

Provided that no order for interception of any communication shall be valid upon the expiry of a period of sixty days from the date of the order.

(2) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed, renew any order for interception of any communication if he is satisfied that the conditions upon which the original order was issued continue to exist.

18. Duty to inform the person concerned. – (1) Subject to sub-section (2), before the expiry of a period of sixty days from the conclusion of any interception of communication ordered or carried out under this Act, the authorised officer who carried out the interception of communication shall, in writing in such form and manner as may be prescribed, notify, with reference to the relevant order of the Chief Privacy Commissioner, each person whose communication was intercepted of the fact of such interception and duration thereof.

(2) The Chief Privacy Commissioner may, on an application made by an authorised officer in such form and manner as may be prescribed, if he is satisfied that the notification under sub-section (1) would –

(a) present a reasonable threat to national security, defence or public order, or
(b) adversely affect the prevention, investigation or prosecution of a cognisable offence,

for reasons to be recorded in writing addressed to the authorised officer, order that the person whose communication was intercepted not be notified of the fact of such interception or the duration thereof:
Provided that no person whose communication was intercepted shall not be notified of the fact of such interception and duration thereof.

19. Security and duty of confidentiality and secrecy. — (1) No person shall intercept any communication of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality and secrecy of all information obtained as a result of an interception of communication, including from theft, loss or unauthorised disclosure.

(2) Any person who carries out any interception of any communication, or who obtains any information, including personal data, as a result of an interception of communication, shall be subject to a duty of confidentiality and secrecy in respect of it.

(3) Every competent organisation shall, before the expiry of a period of one hundred days from the enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively responsible for all interceptions of communications carried out by that competent organisation.

20. Disclosure of intercepted communications. — (1) Save as provided in this section, no person shall disclose to any other person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of an interception of any communication including the fact that the interception of communication was carried out.

(2) Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of an interception of any communication is necessary to –

(a) prevent a reasonable threat to national security, defence or public order, or
(b) prevent, investigate or prosecute a cognisable offence;

an authorised officer may disclose the information, including personal data, obtained as a result of the interception of any communication to any authorised officer of any other competent organisation:

Provided that no authorised officer shall disclose any information, including personal data, obtained as a result of the interception of any communication that is not necessary to achieve the purpose for which the disclosure is sought.

21. Storage of intercepted communications. — (1) Subject to sub-section (2), no person shall store any information, including personal data, obtained as a result of an interception of any communication for a period longer than one hundred and eighty days from the date on which the last order for interception of the communication to which the obtained information pertains expired.

(2) The Chief Privacy Commissioner may, on an application made in such form and manner as may be prescribed, if he is satisfied that it is necessary –

(a) to prevent a reasonable threat to national security, defence or public order, or
(b) to prevent, investigate or prosecute a cognisable offence;

for reasons to be recorded in writing, order that any information, including personal data, obtained as a result of an interception of any communication may be stored for a period longer than one hundred and
eighty days from the date on which the last order for interception of the communication to which the obtained information pertains expired.

CHAPTER V
SURVEILLANCE

22. Bar against surveillance. — Notwithstanding anything contained in any other law for the time being in force, but save as provided in this chapter, no person shall order or carry out, or cause the ordering or carrying out of, any surveillance of another person.

23. Surveillance by the State. — (1) No member of a police force, armed force, intelligence organisation, public authority or the State shall order or carry out, or cause to be ordered or carried out, any surveillance of another person save in pursuance of an order by the Chief Privacy Commissioner or any other person authorised by him in this behalf.
(2) No surveillance shall be ordered or carried out that is not necessary to achieve the purpose for which the surveillance is sought.
(3) Any authorised officer seeking to carry out any surveillance of another person shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.
(4) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, if he is satisfied that the surveillance is necessary —
   (a) to prevent a reasonable threat to national security, defence or public order, or
   (b) to prevent, investigate or prosecute a cognisable offence,
   for reasons to be recorded in writing addressed to the authorised officer, order the surveillance.
(5) Prior to issuing an order for surveillance, the Chief Privacy Commissioner, or any other person authorised by him in this behalf, shall satisfy himself that all other lawful means to acquire the information sought to be obtained as a result of the proposed surveillance have been exhausted and that the proposed surveillance is reasonable, proportionate and not excessive.

24. Surveillance by private persons or entities. — (1) Notwithstanding anything contained in any other law for the time being in force, and without prejudice to the provisions of section 23 of this Act, no person who is not a member of a police force, armed force, intelligence organisation, public authority or the State shall carry out, or cause to be carried out, any surveillance in any public place or in any property or premises that is not in his possession.
(2) Without prejudice to sub-section (1), any person who carries out any surveillance under this section shall be subject to a duty to inform, in such manner as may be prescribed, members of the public of such surveillance.
(3) Any person who carries out any surveillance under this section shall, before the expiry of a period of seven days from when the surveillance was first carried out, report the fact of such surveillance, and reasons thereof, in such form and manner as may be prescribed, to the Chief Privacy Commissioner.

25. Duration of surveillance. — (1) An order for surveillance shall specify the period of its validity and, upon the expiry of the validity of the order, all surveillance carried out in relation to that order shall cease forthwith:
Provided that no order for surveillance shall be valid upon the expiry of a period of sixty days from the date of the order.

(2) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed, renew any order for surveillance if he is satisfied that the conditions upon which the original order was issued continue to exist.

26. Duty to inform the person concerned. — (1) Subject to sub-section (2), before the expiry of a period of sixty days from the conclusion of any surveillance ordered or carried out under this Act, the authorised officer who carried out the surveillance shall, in writing in such form and manner as may be prescribed, notify, with reference to the relevant order of the Chief Privacy Commissioner, each person in respect of whom surveillance was carried out of the fact of such surveillance and duration thereof.

(2) The Chief Privacy Commissioner may, on an application made by an authorised officer in such form and manner as may be prescribed, if he is satisfied that the notification under sub-section (1) would —

(a) present a reasonable threat to national security, defence or public order, or
(b) adversely affect the prevention, investigation or prosecution of a cognisable offence,

for reasons to be recorded in writing addressed to the authorised officer, order that the person in respect of whom surveillance was carried out not be notified of the fact of such surveillance or the duration thereof:

Provided that no person in respect of whom surveillance was carried out shall not be notified of the fact of such surveillance and duration thereof.

27. Security and duty of confidentiality and secrecy. — (1) No person shall carry out any surveillance of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality and secrecy of all information obtained as a result of surveillance, including from theft, loss or unauthorised disclosure.

(2) Any person who carries out any surveillance, or who obtains any information, including personal data, as a result of surveillance, shall be subject to a duty of confidentiality and secrecy in respect of it.

(3) Every police force, armed force, intelligence organisation, public authority or State shall, before the expiry of a period of one hundred days from the enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively responsible for all surveillance carried out:

Provided that a public authority that does not order or carry out surveillance shall not be required to designate any Privacy Officers under this sub-section.

(4) Every person who is not a member of a police force, armed force, intelligence organisation, public authority or State and who seeks to carry out any surveillance shall, at least seven days before the surveillance is first carried out, designate or appoint as many persons as it deems fit as Privacy Officers who shall be responsible for all surveillance carried out:
Provided that where surveillance is carried out by a single person, that person shall be deemed to be a Privacy Officer.

28. Disclosure of surveillance. – (1) Save as provided in this section, no person shall disclose to any other person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of any surveillance including the fact that the surveillance was carried out.

(2) Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of surveillance is necessary to –

(a) prevent a reasonable threat to national security, defence or public order, or
(b) prevent, investigate or prosecute a cognisable offence,

that information, including personal data, obtained as a result of surveillance may be disclosed to a police force, armed force, intelligence organisation, public authority or State only:

Provided that no person shall disclose any information, including personal data, obtained as a result of surveillance that is not necessary to achieve the purpose for which the disclosure is sought.

29. Storage of surveillance. – (1) Subject to sub-section (2), no person shall store any information, including personal data, obtained as a result of surveillance for a period longer than one hundred and eighty days from the date on which the surveillance to which the obtained information pertains ceased.

(2) The Chief Privacy Commissioner may, on an application made in such form and manner as may be prescribed, if he is satisfied that it is necessary –

(a) to prevent a reasonable threat to national security, defence or public order, or
(b) to prevent, investigate or prosecute a cognisable offence,

for reasons to be recorded in writing, order that any information, including personal data, obtained as a result of surveillance may be stored for a period longer than one hundred and eighty days from the date on which the last order for surveillance to which the obtained information pertains expired.

CHAPTER VI

THE PRIVACY COMMISSION

30. Constitution of the Privacy Commission. – (1) The Central Government shall, by notification, constitute, with effect from such date as may be specified therein, a body to be called the Privacy Commission consisting of a Chief Privacy Commissioner and not more than six other Privacy Commissioners, to be appointed by the President, by warrant under his hand and seal, to exercise the jurisdiction and powers and discharge the functions and duties conferred or imposed upon them by or under this Act.

(2) The Chief Privacy Commissioner shall be a person who has been a Judge of the Supreme Court:
Provided that the appointment of the Chief Privacy Commissioner shall be made only after consultation with the Chief Justice of India.

(3) One Privacy Commissioner shall be a person who is or has been a Judge of a High Court:

Provided that no sitting Judge of a High Court shall be appointed except after consultation with the Chief Justice of India.

(4) One Privacy Commissioner shall be a person of ability, integrity and standing who has a special knowledge of, and professional experience of not less than ten years in privacy law and policy.

31. Term of office, conditions of service, etc. of Chief Privacy Commissioner and Privacy Commissioners. — (1) Before appointing any person as the Chief Privacy Commissioner or Privacy Commissioner, the President shall satisfy himself that the person does not, and will not, have any such financial or other interest as is likely to affect prejudicially his functions as such Chief Privacy Commissioner or Privacy Commissioner.

(2) The Chief Privacy Commissioner and every Privacy Commissioner shall hold office for such period, not exceeding five years, as may be specified by the President in the order of his appointment, but shall be eligible for reappointment:

Provided that no person shall hold office as the Chief Privacy Commissioner or Privacy Commissioner after he has attained the age of sixty-seven years.

(3) Notwithstanding anything contained in sub-section (2), the Chief Privacy Commissioner or any Privacy Commissioner may—

(a) by writing under his hand and addressed to the President resign his office at any time;
(b) be removed from office in accordance with the provisions of section 32 of this Act.

(4) A vacancy caused by the resignation or removal of the Chief Privacy Commissioner or Privacy Commissioner under sub-section (3) shall be filled by fresh appointment.

(5) In the event of the occurrence of a vacancy in the office of the Chief Privacy Commissioner, such one of the Privacy Commissioners as the President may, by notification, authorise in this behalf, shall act as the Chief Privacy Commissioner till the date on which a new Chief Privacy Commissioner, appointed in accordance with the provisions of this Act, to fill such vacancy, enters upon his office.

(6) When the Chief Privacy Commissioner is unable to discharge his functions owing to absence, illness or any other cause, such one of the Privacy Commissioners as the Chief Privacy Commissioner may authorise in writing in this behalf shall discharge the functions of the Chief Privacy Commissioner, till the date on which the Chief Privacy Commissioner resumes his duties.

(7) The salaries and allowances payable to and the other terms and conditions of service of the Chief Privacy Commissioner and Privacy Commissioners shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Chief Privacy Commissioner and any Privacy Commissioner shall be varied to his disadvantage after his appointment.
(8) The Chief Privacy Commissioner and Privacy Commissioners ceasing to hold office as such shall not hold any appointment under the Government of India or under the Government of any State for a period of five years from the date on which he ceases to hold such office.

32. Removal of Chief Privacy Commissioner and Privacy Commissioners from office in certain circumstances. – (1) The President may remove from office the Chief Privacy Commissioner or any Privacy Commissioner, who –

(a) is adjudged an insolvent; or
(b) engages during his term of office in any paid employment outside the duties of his office; or
(c) is unfit to continue in office by reason of infirmity of mind or body; or
(d) is of unsound mind and stands so declared by a competent court; or
(e) is convicted for an offence which in the opinion of the President involves moral turpitude; or
(f) has acquired such financial or other interest as is likely to affect prejudicially his functions as a Chief Privacy Commissioner or Privacy Commissioner, or
(g) has so abused his position as to render his continuance in office prejudicial to the public interest.

(2) Notwithstanding anything contained in sub-section (1), neither the Chief Privacy Commissioner nor any Privacy Commissioner shall be removed from his office on the ground specified in clause (f) or clause (g) of that sub-section unless the Supreme Court on a reference being made to it in this behalf by the President, has on an inquiry held by it in accordance with such procedure as it may specify in this behalf, reported that the Chief Privacy Commissioner or Privacy Commissioner ought, on such grounds, to be removed.

33. Functions of the Privacy Commission. – (1) The Privacy Commission may inquire, suo moto or on a petition presented to it by any person or by someone acting on his behalf, in respect of any matter connected with the collection, storage, processing, disclosure or other handling of any personal data, interception of any communication, or surveillance of any person, and give such directions or pass such orders as are necessary for reasons to be recorded in writing.

(2) Without prejudice to the generality of the foregoing provision, the Privacy Commission shall perform all or any of the following functions, namely –

(a) review the safeguards provided by or under this Act and other law for the time being in force for the protection of privacy and recommend measures for their effective implementation;
(b) review any measures taken by any competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity for the protection of privacy and take such further action as it deems fit;
(c) review any action, policy or procedure of any competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to ensure compliance with this Act and any rules made hereunder;
(d) formulate, in consultation with experts, norms for the effective protection of privacy by competent organisations, police forces, armed forces, intelligence organisations, public authorities, companies, persons or other entities;
(e) promote awareness and knowledge of privacy rights and obligations through any means necessary;
(f) undertake and promote research in the field of privacy rights;
(g) encourage the efforts of non-governmental organisations and institutions working in the field of privacy rights;
(h) publish periodic reports concerning the incidence of collection, processing, storage, disclosure and other handling of personal data, interception of communications and surveillance;
(i) such other functions as it may consider necessary for the protection and promotion of privacy.

(3) Subject to the provisions of any rules prescribed in this behalf by the Central Government, the Privacy Commission shall have the power to review any decision, judgement, decree or order made by it.
(4) In the exercise of its functions under this Act, the Privacy Commission shall give such directions or pass such orders as are necessary for reasons to be recorded in writing.
(5) The Privacy Commission may, in its own name, sue or be sued.

34. Secretary, officers and other employees of the Privacy Commission. – (1) The Central Government shall appoint a Secretary to the Privacy Commission to exercise and perform, under the control of the Chief Privacy Commissioner such powers and duties as may be prescribed or as may be specified by the Chief Privacy Commissioner.
(2) The Central Government may provide the Privacy Commission with such other officers and employees as may be necessary for the efficient performance of the functions of the Privacy Commission.
(3) The salaries and allowances payable to and the conditions of service of the Secretary and other officers and employees of the Privacy Commission shall be such as may be prescribed.

35. Salaries, etc. be defrayed out of the Consolidated Fund of India. – The salaries and allowances payable to the Chief Privacy Commissioner and Privacy Commissioners and the administrative expenses, including salaries, allowances and pension, payable to or in respect of the officers and other employees of the Privacy Commission shall be defrayed out of the Consolidated Fund of India.

36. Vacancies, etc. not to invalidate proceedings of the Privacy Commission. – No act or proceeding of the Privacy Commission shall be questioned on the ground merely of the existence of any vacancy or defect in the constitution of the Privacy Commission or any defect in the appointment of a person acting as the Chief Privacy Commissioner or Privacy Commissioner.

37. Chief Privacy Commissioner, Privacy Commissioners and employees of the Privacy Commission to be public servants. – The Chief Privacy Commissioner and Privacy Commissioners and other employees of the Privacy Commission shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code, 1860.
38. Location of the office of the Privacy Commission. – The offices of the Privacy Commission shall be in New Delhi or any other location as directed by the Chief Privacy Commissioner in consultation with the Central Government.

39. Procedure to be followed by the Privacy Commission. – (1) Subject to the provisions of this Act, the Privacy Commission shall have powers to regulate –

(a) the procedure and conduct of its business;
(b) the delegation to one or more Privacy Commissioners of such powers or functions as the Chief Privacy Commissioner may specify.

(2) In particular and without prejudice to the generality of the foregoing provisions, the powers of the Privacy Commission shall include the power to determine the extent to which persons interested or claiming to be interested in the subject-matter of any proceeding before it may be allowed to be present or to be heard, either by themselves or by their representatives or to cross-examine witnesses or otherwise take part in the proceedings:

Provided that any such procedure as may be prescribed or followed shall be guided by the principles of natural justice.

40. Power relating to inquiries. – (1) The Privacy Commission shall, for the purposes of any inquiry or for any other purpose under this Act, have the same powers as vested in a civil court under the Code of Civil Procedure, 1908, while trying suits in respect of the following matters, namely –

(a) the summoning and enforcing the attendance of any person from any part of India and examining him on oath;
(b) the discovery and production of any document or other material object producible as evidence;
(c) the reception of evidence on affidavit;
(d) the requisitioning of any public record from any court or office;
(e) the issuing of any commission for the examination of witnesses; and,
(f) any other matter which may be prescribed.

(2) The Privacy Commission shall have power to require any person, subject to any privilege which may be claimed by that person under any law for the time being in force, to furnish information on such points or matters as, in the opinion of the Privacy Commission, may be useful for, or relevant to, the subject matter of an inquiry and any person so required shall be deemed to be legally bound to furnish such information within the meaning of section 176 and section 177 of the Indian Penal Code, 1860 (45 of 1860).

(3) The Privacy Commission or any other officer, not below the rank of a Gazetted Officer, specially authorised in this behalf by the Privacy Commission may enter any building or place where the Privacy Commission has reason to believe that any document relating to the subject matter of the inquiry may be found, and may seize any such document or take extracts or copies therefrom subject to the provisions of section 100 of the Code of Criminal Procedure, 1973 (2 of 1974), in so far as it may be applicable.
(4) The Privacy Commission shall be deemed to be a civil court and when any offence as is described in section 175, section 178, section 179, section 180 or section 228 of the Indian Penal Code, 1860 (45 of 1860) is committed in the view or presence of the Privacy Commission, the Privacy Commission may, after recording the facts constituting the offence and the statement of the accused as provided for in the Code of Criminal Procedure, 1973 (2 of 1974), forward the case to a Magistrate having jurisdiction to try the same and the Magistrate to whom any such case is forwarded shall proceed to hear the complaint against the accused as if the case had been forwarded to him under section 346 of the Code of Criminal Procedure, 1973.

41. Decisions of the Privacy Commission. – (1) The decision of the Privacy Commission shall be binding.

(2) In its decision, the Privacy Commission has the power to –

(a) require a competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to take such steps as may be necessary to secure compliance with the provisions of this Act;

(b) require a competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to compensate any person for any loss or detriment suffered;

(c) impose any of the penalties provided under this Act.

42. Proceedings before the Privacy Commission to be judicial proceedings. – The Privacy Commission shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 and every proceeding before the Privacy Commission shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228 and for the purposes of section 196 of the Indian Penal Code, 1860.

CHAPTER VII
OFFENCES AND PENALTIES

43. Punishment for offences related to personal data. – (1) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes or otherwise handles any personal data shall be punishable with imprisonment for a term which may extend to [___] years and may also be liable to fine which may extend to [___] rupees.

(2) Whoever attempts to commit any offence under sub section (1) shall be punishable with the punishment provided for such offence under that sub-section.

(3) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes or otherwise handles any sensitive personal data shall be punishable with imprisonment for a term which may extend to [increased for sensitive personal data] years and may also be liable to fine which may extend to [___] rupees.

(4) Whoever attempts to commit any offence under sub section (3) shall be punishable with the punishment provided for such offence under that sub-section.

44. Punishment for offences related to interception of communication. – (1) Whoever, except in conformity with the provisions of this Act, intercepts, or causes the interception of, any communication
of another person shall be punishable with imprisonment for a term which may extend to [____] years and may also be liable to fine which may extend to [____] rupees.

(2) Whoever attempts to commit any offence under sub section (1) shall be punishable with the punishment provided for such offence under that sub section.

45. Punishment for offences related to surveillance. – (1) Whoever, except in conformity with the provisions of this Act, orders or carries out, or causes the ordering or carrying out, of any surveillance of another person shall be punishable with imprisonment for a term which may extend to [____] years and may also be liable to fine which may extend to [____] rupees.

(2) Whoever attempts to commit any offence under sub section (1) shall be punishable with the punishment provided for such offence under that sub section.

46. Abetment and repeat offenders. – (1) Whoever abets any offence punishable under this Act shall, if the act abetted is committed in consequence of the abetment, be punishable with the punishment provided for that offence.

(2) Whoever, having been convicted of an offence under any provision of this Act is again convicted of an offence under the same provision, shall be punishable, for the second and for each subsequent offence, with double the penalty provided for that offence.

47. Offences by companies. – (1) Where an offence under this Act has been committed by a company, every person who, at the time of the offence was committed, was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section (1), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall be deemed to be guilty of that offence, and shall be liable to be proceeded against and punished accordingly.

48. Cognisance. – Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offences under sub-section (3) of section 43, section 44, section 45 and section 46 shall be cognisable and non-bailable.

49. General penalty. – Whoever, in any case in which a penalty is not expressly provided by this Act, fails to comply with any notice or order issued under any provisions thereof, or otherwise contravenes any of the provisions of this Act, shall be punishable with fine which may extend to [____] rupees, and, in the case of a continuing failure or contravention, with an additional fine which may extend to [____] rupees for every day after the first during which he has persisted in such failure or contravention.
50. Punishment to be without prejudice to any other action. — The award of punishment for an offence under this Act shall be without prejudice to any other action which has been or which may be taken under this Act with respect to such contravention.

CHAPTER VIII
MISCELLANEOUS

51. Power to make rules. — (1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for —

(a) the notification of theft, loss or damage under sub-section (3) of section 9;
(b) the order in writing from an officer-in-charge of a police station under sub-section (5) of section 10;
(c) the notification of disclosure under sub-section (5) of section 10;
(d) the application by an intelligence organisation under sub-section (2) of section 13;
(e) the application to intercept a communication under sub-section (1) of section 15;
(f) the application to renew an interception of communication under sub-section (2) of section 17;
(g) the notification of an interception of communication under sub-section (1) of section 18;
(h) the application to not inform under sub-section (2) of section 18;
(i) the application to store information obtained as a result of any interception of communication under sub-section (2) of section 21;
(j) the application to carry out surveillance under sub-section (3) of section 23;
(k) notification to the general public under sub-section (2) of section 24;
(l) the reporting of surveillance under sub-section (3) of section 24;
(m) the application to renew surveillance under sub-section (2) of section 25;
(n) the notification of surveillance under sub-section (1) of section 26;
(o) the application to not inform under sub-section (2) of section 26;
(p) the application to store information obtained as a result of surveillance under sub-section (2) of section 29;
(q) salaries, allowances and other terms and conditions of service of the Chief Privacy Commissioner, Privacy Commissioners, Secretaries and other members, staff and employees of the Privacy Commission;
(r) procedure to be followed by the Privacy Commission;
(s) powers and duties of Secretaries, officers and other employees of the Privacy Commission;
(t) the effective implementation of this Act.

(3) Every rule made under this section shall be laid, as soon as may be after it is made, before each House of Parliament while it is in session for a period of thirty days which may be comprised in one session or in two successive sessions and if before the expiry of the session in which it is so laid or the session immediately following, both Houses agree in making any modification in the rule, or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or
be of no effect, as the case may be, so however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

52. **Bar of jurisdiction.** – (1) On and from the appointed day, no court or authority shall have, or be entitled to exercise, any jurisdiction, powers or authority (except the Supreme Court and a High Court exercising powers under Articles 32, 226 and 227 of the Constitution) in relation to matters specified in this Act.

(2) No order passed under this Act shall be appealable except as provided therein and no civil court shall have jurisdiction in respect of any matter which the Privacy Commission is empowered by, or under, this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

53. **Protection of action taken in good faith.** – No suit or other legal proceeding shall lie against the Central Government, State Government, Privacy Commission, Chief Privacy Commissioner, Privacy Commissioner or any person acting under the direction either of the Central Government, State Government, Privacy Commission, Chief Privacy Commissioner or Privacy Commissioner in respect of anything which is in good faith done or intended to be done in pursuance of this Act or of any rules or any order made thereunder.

54. **Power to remove difficulties.** – (1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions, not inconsistent with the provisions of this Act, as appears to it to be necessary or expedient for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of a period of three years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

55. **Act to have overriding effect.** – The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.
EMERGING TRENDS OF THE RIGHT TO PRIVACY

Lakhwinder Singh*

(1) INTRODUCTION

In the contemporary world, we all are under 24*7 surveillance of Big Brother camera. At the same point of time, everyone has the reasonable expectation of privacy, towards which the government, social institutions and any individual must show the adequate respect.

Although the word “Right to Privacy” was firstly tossed up by Samuel D. Warren and Louis D. Brandeis in 1890 in the form of “right to be let alone” and finally got the constitutional status in Griswold v. Connecticut\textsuperscript{1} but it is an inherent right.

On our planet, all living organisms take birth with the sense of self-protection. It is manifested with the fact that no one wants to intrude anybody into his physical privacy. In fact, after the delve study, the anthropologists have deciphered the fact that both animals and human beings share some common mechanisms in protecting their private spheres of life.\textsuperscript{2}

But human beings are blessed with the sixth sense, and hence, with the increase in the human reasoning and knowledge, a ‘man’ has developed the concept of “privacy’. In consequence to this, the shift took place from mere ‘physical privacy’ to ‘psychological privacy’ or ‘mental privacy’ and the ‘modern state’ is under the obligation to protect both of them. In every religious precinct, the importance has been given to ‘privacy’ so that spiritual consciousness should be achieved. More or less every religion recognizes the value of privacy.

According to Alan F. Westin\textsuperscript{3}, the functions of privacy in democratic societies can be grouped under the following headings: (a) personal autonomy (b) Emotional release (c) Self-evaluation and (d) Limited and Protected communication.

* Research Scholar, Department of Laws, Panjab University Chandigarh.

\textsuperscript{1} 381 U.S. 47 (1965)
\textsuperscript{2} Alan F. Westin, Privacy and Freedom, at 8 (1970).
\textsuperscript{3} Id. at at 32
According to Alan F. Westin, Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.  

The interests in privacy protected under common law are classified into four by Prosser.

1. Intrusion upon plaintiff’s seclusions or solitude.
2. Public disclosure of embarrassing facts.
3. Publicity which places the plaintiff in false right.
4. Appropriation for defendant’s advantages, of plaintiff’s name and likeness.

(2) PRIVACY AND RELIGION

Milton Konvitz has called attention to ways in which biblical passages can be interpreted as distinguishing a realm of privacy:

Almost the first page of the Bible introduces us to the feeling of shame as a violation of privacy. After Adam and Eve had eaten the fruit of the tree of knowledge, "the eyes of both were opened, and they knew that they were naked; and they sewed fig leaves together and made themselves aprons." Thus, mythically, we have been taught that our very knowledge of good and evil - our moral nature as men is somehow, by divine ordinance, linked with a sense and realm of privacy.

The frequent use of words like Ekant, Rahasaya, Tiraskarinee, Avagunthanvatee Naree and their synonyms in the Indian scriptures and classical literature, it cannot be maintained that privacy was alien to ancient Indian culture. Even the importance of privacy and solitude is being attached to the process of meditation. Lord Shiva, while, in meditation, is said to have been disturbed by Kamadeva, the god of love and sex in the Indian mythology, who was burnt as punishment therof when Lord Shiva opened his third eye.

Islam gives great importance to the fundamental human right to privacy. Islamic Shariah fully acknowledges the sanctity of the privacy of one’s home and private life, and there is ample admonition against prying into the affairs of others. The principles of Islam

---

1. Id. at 7
2. Prosser, “Privacy” 38 Col. L. Rev. 383 (1960)
5. Ibid.
elevate the religious conscience of every Muslim, and protection of the privacy of every Muslim lies at the core of Islamic principles. Islamic jurisprudence requires strict caution in such matters affecting people’s lives, honor (sanctity) and right to property. Islam orders that one should not inquire into private matters of others, and strictly prohibits prying into these matters. If someone happens to come across private information, further disclosure of that information is not permitted. Managing the affairs of the private domain is the exclusive right of the individual.9

(3) EVOLUTION OF THE RIGHT TO PRIVACY
The modern version of the right to privacy was initially brought up by the Samuel D. Warren and Louis D. Brandeis in 1890 in the form of the right to be let alone. In 1890, two Boston lawyers, Samuel D. Warren and Louis D. Brandeis, published a joint article, “The Right to Privacy” in the very young Harvard Law Review. This article became very influential and Roscoe Pound said that it did nothing less than add a chapter to the law.10

It was said to have been provoked by press publicity of which Warren and his family were the unhappy victims. It came at a time when, as the authors complained, a developing technology made it possible to intrude upon private lives and activities and to expose them to public gaze for reasons no better than mere titillation and vulgar curiosity.11

Basically this article was published against the wide spread of yellow journalism and unregulated use of mechanical bug devices.

In this article the authors observed that in old times, the law gave a remedy only for the physical interference with life and property. Right to life was confined only to the protection from battery and liberty meant freedom from actual restraint. Later, there came recognition of man’s spiritual nature, of his feelings and his intellect.12

Thus, with the recognition of the legal value of human sensations, the law of assault, nuisance, Defamation, etc. was developed.13

In their contemporary society, the authors observed that with the new scientific inventions and business methods, the individual privacy is in danger. Instantaneous

---


11 Ibid.
13 Id. at 194
photographs, newspaper enterprises and the mechanical bug devices had invaded the sacred precincts of private and domestic life. Therefore, they were in the favour securing to the individual what Judge Cooley called the “right to be let alone”.14

The second alarm was again ringed by Louis Brandeis as a Justice of the Supreme Court of United States. In Olmstead v. United States15, he gave his dissenting opinion against the court’s verdict. In this case, the Court held that phone-tapping does not amount to physical trespass into the home and hence not violative of the Fourth and Fifth Amendments.

Justice Holmes in a celebrated phrase characterized wiretapping as “dirty businesses”. Brandeis went further; he anticipated the development of a technology which would give government the capacity to pry into the deepest recesses of the lives of individuals, and it was against this threat protection had to be provided.16 Therefore, according to Justice Brandeis, any evidence which has been obtained through unauthorized phone-tapping is not admissible.

Justice Brandeis observed 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.17

In Katz v. United States,18 the Court adopted Brandeis’s view, overruling Olmstead. 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.19

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.20

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.21 But it was not until 1965

14 Id. at 195
15 277 US 438 (1927)
16 supra note 10 at 87
17 supra note 15 at 478
20 Id. at 1102
21 M. Glenn Abernathy, Civil Liberties under the Constitution, at 95 (1977).
that the US Supreme Court squarely held that the Constitution contained at least a limited right to privacy.\(^{22}\)

In *Griswold v. Connecticut*\(^{23}\), the right to privacy got the constitutional status. The court invalidated the statute which made it a criminal offense for a married couple to use contraceptives because it is an invasion into their right to privacy. And the court further held that “the right to privacy” as a right older than the Bill of Rights.\(^{24}\) The court held that the various guaranties contained in the Bill of Rights, such as First, Third, Fourth, Fifth and Ninth Amendments creates the “zone of Privacy”\(^{25}\).

In *Roe v. Wade*\(^{26}\), the court struck down a Texas statute which prohibited almost all abortions. The court held that right to privacy is broad enough to encompass a woman’s decision whether or not to terminate her pregnancy.\(^{27}\)

### (4) MEDIA AND PRIVACY

The investigative journalism which received a boost after the Watergate disclosures in the U.S.A. has opened an interesting and attractive chapter in the history of the Press throwing denting challenges to the adventurous and the ambitious. It has made the press more powerful and awesome and when handled circumspectly, has helped furbish the image of the Press as an active watchdog of the interests of the society.\(^{28}\)

The carrying out of a sting operation may be an expression of the right to free press but it caries with it an indomitable duty to respect the privacy of others. The individual who is the subject of a press or television ‘item’ has his or her personality, reputation or career dashed to the ground after the media exposure. He too has a fundamental right to live with dignity and respect and a right to privacy guaranteed to him under Article 21 of the Constitution.\(^{29}\)

---

\(^{22}\) *Ibid.*

\(^{23}\) 14 L. ed 2d 510 (1965).

\(^{24}\) *Id.* at 512

\(^{25}\) *Id.* at 515

\(^{26}\) 35 L. Ed 2d 147 (1973).

\(^{27}\) *Id.* at 177


Today, it is being witnessed that the over-inquisitive media, which is a product of over-commercialization, is severely encroaching the individual’s right to privacy by crossing the boundaries of its freedom.30

Of course, the law does not always give redress in defamation for a true statement. Privacy arises in different circumstances. It is concerned with the publication of private affairs, e.g., details of illness or disease or disease of a person, affairs of a couple on honeymoons, or photograph of a film actress taking a sun-bath. The grievance here is not an injury to reputation. It is injury to feelings. In such an action truth would not be an appropriate defence because the right of privacy implies the right not merely to prevent the inaccurate portrayal of private life but the right to prevent its being depicted at all.31

Probably no event in recent history has had more to say about privacy and private lives than the death of Princess Diana. Although the direct cause of the car accident that killed her is yet unknown, it is clear in the public’s mind that an indirect cause of her death was the incessant invasion of her private space by paparazzi and tabloid journalists.32 More recently, the photograph of Barack Obama, in which it looks like that he casts sly glance at a teenage girl at the G-8 Summit, became very sensitive matter.

In the present era, the media has forgotten its social responsibility and has sold its ethics as well. Under the protective shield of investigative journalism, the media channels are showing the salacious and indecent things. Therefore, the infringement of public morality and decency is more or less amounts to the violation of the mental privacy of the people.

(5) ADVANCEMENT IN TECHNOLOGY AND DATA PRIVACY

The capacity of new media to support the collection, use and storage of vast amounts of personal information by business and governments has underpinned debates on the need to build mechanisms which protect the privacy of individuals using the internet and other technologies. Use of technologies including cookies and web bugs to track behaviour across the web, and the increasing capacity to profile consumers using data gathered from purchases and page accesses, have encouraged the development of international agreements, including the safe Harbor arrangement between the European Union and United States, to manage the use of and trade in personal information. The traditional notions of privacy have been curtailed by the development and application of new technologies to the collection and

30 Ibid.
31 E.S. Venkatarmiah, Freedom of Press, some recent trends, at 112 (1987)
monitoring of personal information by both commercial interests and governments. The internet and interactive media permit business and government to track and monitor individual behaviour, in ways that would have been previously impossible for even the most authoritarian regime, through the establishment of databases, data-mining techniques, and the application of e-mail monitoring and interception technologies including the “Carnivore” system utilized by US security agencies.33 Equally, governments and businesses have sought to adopt technological and procedural measures including web seals and encryption to protect information they have collected from unauthorized access and use.34

Personal information can be collected any time someone writes a cheque, uses a credit or debit card, engages in a financial transaction views world wide web pages, or does anything else that generates a data trial and it includes names, telephone numbers, marital status, education level, job history, credit history, medical records, and any other information that can be linked to specific persons or data subjects. Often, individuals have little choice but to reveal this information, which is collected without their consent or knowledge, or is a by product of a sale or service transaction. Furthermore, personal information can became the basis for decisions made about an individual by others, such as whether someone is offered a job, targeted for government surveillance or eligible for medical insurance.35

Social network sites are the important aspect of the new media. In this virtual world, people use to express their feelings and happenings of the real world. All users voluntarily upload their family pictures, videos, etc on the sites like Youtube, Facebook, etc. and blog about their private matters on sites like Twitter. Majority of the users don’t know even the repercussions of such a usage. These social network sites collect and collate the individual data and sell it to other companies. Finally, such an individual data is being used for commercial purposes like Target-marketing, etc.

The information, posted to social media may be detrimental to users’ privacy and reputation. Numerous media stories report the loss of jobs, college admissions, or relationships due to the posting of photos taken in different states of intoxication.36

34 Id. at 315
Moreover, certain information posted on social networking sites is publicly available to users and non-users alike, and is even searchable by search engines such as Google. But it does not mean that the users don't care about their privacy. They still have reasonable expectations of privacy. The problem is the lack of knowledge regarding the new technologies. The users often hurriedly adopt new social media tools without considering the capacity and potentiality of service providers’ to collect the personal data of its users.38

Therefore, social media must convey to users the essence and consequences of their choices, and clarify the tradeoff between publicity and privacy, in order to enable them to make free and informed choices.39

The current international legal framework for data protection and privacy is founded on instruments such as the 1980 OECD Guidelines and the European Union Data Protection Directive that date from the 1980s and 1990s. At the time these instruments were drafted, technologies that have become pervasive today (such as the Internet, social networking, biometrics, etc.) were virtually unknown. Therefore, such regulations are not compatible with the new techno-world in which everyone’s privacy is at stake. Thus, new governance on the online technologies is required.40

The story doesn’t stop here. Nowadays, all the governments are using advanced technologies like Biometrics, facial recognition, GPS, CCTV, Satellite monitoring, smart dust, etc. for the purpose of security. And these technologies are being used on large scale after 9/11 attacks and recently Mumbai attacks.

Basically, the Government collects the personal information of its citizens for the security of the State, to prevent tax evasion or for any other public good. And people trust the government that their personal information will be protected. But recently in Dec. 2010, the exposure of Radia tapes at T.V. News Channel, has breached the trust of Indian Citizens. Ratan Tata moved to the Hon’ble Supreme Court on the ground that what was his personal information was collected by government through phone tapping has been disclosed by the media and the government has failed to protect the data of his personal information.

It is generally observed that whenever terrorist attacks occurred like 9/11 and Mumbai attacks, people’s concern for their security is also increased. And this concern reflects their approval for governmental investigative powers. Thus, government’s surveillance power also

---

37 Id. at 24
38 Id. at 25
39 Ibid.
40 Id at 15
increases. But it is submitted that such power should not be abused otherwise it amounts to the breach of public trust.

Today, the all-seeing eye need not necessarily belong to the government, as many in the private sector find it valuable to conduct various forms of surveillance or to “mine” data collected by others. For example, employers continually seek new ways to monitor employees for efficiency and honesty; firms trawl databases for preference information in the search for new customers. With the technological developments, the costs of data collection and surveillance will decrease, while the quantity and quality of data will increase.

Recently highlighted facts of pat-down searches and electronic surveillance again increased the threat to individual privacy. Especially, pat-down searches by security agents amount to sexual assaults.

Sense-enhanced searches rely on one or more technologies to detect that which ordinarily could not be detected with un-aided human senses. Sense-enhanced searches allow someone on the outside to see what is happening inside a building, a package, or even clothing. Sense enhanced search technology is changing rapidly, raising doubts as to what constitutes a reasonable expectation of privacy in a world where we are all increasingly naked and living in transparent homes. Governments appear to be the primary users of sense-enhanced searches, but many of the technologies are moving into the private sector as prices decrease.

The devices which can see through the clothes are being used as an alternative to pat-down searches at Airports.

However, according to Jeffrey Rosen, Professor at George Washington University Law, there is a better alternative than the full body scans. Dutch airports use a different technology that does not Project an image unless a suspicious material is found. Only the area of suspicion is revealed and the rest of the body is “blob-like human image.” US officials have said the alternative technology produces a high rate of false positives. Even so, Rosen suggests false positives leading to pat down searches maybe less intrusive than U.S. machines projecting full body images and the full pat-downs performed on those who object. Full body

\[^{43}\text{Id. at 1496}\]
scanners are capable of recording and storing images when it ‘test’ mode. U.S. officials have said the images are not being recorded or stored, but Rosen fear abuses.44

The modern bio-medical technologies impinge privacy aspects of an individual in a variety of ways. One of them is genetic information which is a medical record and the doctor has a duty to maintain confidentiality of patient’s health record. Genetic information is the heritable biological information. It can be used as the basis for insidious discrimination. Unfortunately, the employers and the insurance companies have been gaining access to genetic information for deciding employability and insurability respectively.45

(6) PRIVACY IN INDIA

The concept of privacy was not alien to ancient India. Right to privacy was initially practiced as a custom. Among various customs, there was the norm of the seclusion of women from the male stranger’s gaze. This custom of privacy had its foundation laid in the rules regulating the construction of houses. The earliest mention of such rules is found in the Kautilya’s Arthashastra wherein the violation of such rules was made punishable.46 By considering the importance of these customs, the Britishers initially recognized the right to privacy as a customary right and thereafter as a statutory right.

In the post-independent India, “right to privacy” was nowhere mentioned in the Constitution of India. It was the judiciary only who invented the right to privacy in India and gave it the constitutional status. The Hon’ble Supreme Court of India was greatly influenced by the decisions of American Supreme Court and hence found the right to privacy in Article 21 by construing it liberally.

Initially the right to privacy was developed by spelling it out from the right to freedom of speech and expression in Art 19(1)(a) and the right to ‘life’ in Art. 21.47 The initial two cases i.e. Kharak Singh’s case and Govind’s case, decided by the Supreme Court of India where the foundations for the right were laid, concerned the intrusion into the home by the police under State regulations, by way of ‘domiciliary visits’.48

45 Supra note 7 at 383
46 Supra note 7 at 82.
47 District Registrar & Collector, Hyderabad v. Canara Bank AIR 2005 SC 186 at 196
48 Ibid.
In People’s Union for Civil Liberties v. Union of India\textsuperscript{49}, the Supreme Court held that wiretaps were a “serious invasion of an individual’s privacy.” The court also set out guidelines for wiretapping by the government defining how phones may be tapped and under what circumstances. The right is only available to the State and not to private entities.

Recently in Selvi v. State of Karnataka\textsuperscript{50}, the Supreme Court held that compulsory administration of any of the techniques, like narcoanalysis, polygraph examination and brain Electrical Activation Profile (BEAP) test, is an unjustified intrusion into the mental privacy of an individual.\textsuperscript{51} It was also recognized that forcible intrusion into a person’s mental processes is also an affront to human dignity and liberty, often with grave and long-lasting consequences.\textsuperscript{52}

The most significant development outside search and surveillance issues is the decision of the High Court of Delhi in Naz Foundation v. Government of NCT of Delhi. The broadest statement of the Delhi High court’s approach, following its review of Indian case law on protection of privacy, is “The right to privacy thus has been held to protect a “private space in which man may become and remain himself”. The ability to do so is exercised in accordance with individual autonomy.”

Therefore, the approach of the Supreme Court is now towards the protection of individual privacy. By giving more and more personal autonomy to the individual, the Supreme Court also protecting his decisional privacy. In fact in Khushboo’s case also, the court recognized the Live-in relationships which is again a right of decisional privacy. The rigid attitude of the courts against honour-killings is the step towards the protection of one’s right to choose his or life partner.

Nowadays another facet of privacy i.e. informational or data privacy has become the buzzword in India. Our country is planning to draft the Data Protection law but it is very embryonic stage. India is a fast growing economy and its data protection law is a great concern for the international outsourcing of processing of personal information i.e. BPO’s. India is planning to introduce a biometric-based ID system by 2011, to be issued to its 1.2 billion citizens. It is to be implemented by a newly-established Unique Identification Authority of India (UIDAI) established in Feb. 2009, the operation of which will change the significance of all other personal information processing in India, particularly if and when

\textsuperscript{49} (1997) 1 SCC 301
\textsuperscript{50} 2010(4) SCALE 690
\textsuperscript{51} Id. at 783
\textsuperscript{52} Id. at 778
\textsuperscript{53} Cited in Graham Greenleaf, “Promises and illusions of data protection in Indian law”, International Data Privacy Law, 2011, vol.1, No.1, 47-69 at 49
linked to the National Population register (NPR) and the National intelligence grid (NATGRID).54 The existing laws for the protection of individual data are not sufficient. In particular, the key data protection provisions of the 2008 amendments to the Information Technology Act 2000 are not yet effective, and the consumer protections in the credit reporting legislation appear to be ignored by regulators and credit bureaux alike.55

Although the cases on Article 21 have not yet involved data protection issues, the Indian legal system is open to such judicial intervention, as illustrated by the Supreme Court’s development of a right of access to public information prior to its national enactment in the Right to Information Act 2005. If the legislature has failed to enact protections required by the Constitution, the Supreme Court can make binding rules which will operate until laws are made by the legislature and found by the court to be sufficient. The possibility of judicial developments must be kept in mind when considering the scope of Indian data protection law.56

(7) CONCLUSIONS AND SUGGESTIONS

It has been recognized at all levels of the society that right to privacy is an inherent right and is inviolable. With the growth of the industrialization, globalization and liberalization, the shift has come from joint privacy to individual privacy. With overreaching powers of media and increase in the privacy destroying techniques individual privacy is at stake. In this cyber age, the government has the potential to collect all personal details of every individual for any public purpose. But with the decrease in the cost of technology, private entities are also using very sophisticated privacy destroying technologies. Present law is insufficient to tackle these problems.

It is submitted that media should not forget its social responsibility. Investigative journalism is a potent tool of the freedom of press and media and should be used for the public good. Media is also bound towards code of ethics. Whenever the personal data has been stored by the authorized entities, the concerned individual must know its purpose. Such personal data should be used for that purpose only for which it has been stored and should be properly protected. In order to do so an effective Data Protection Law is required.

54 Graham Greenleaf, “Promises and illusions of data protection in Indian law”, International Data Privacy Law, 2011, vol. 1, No. 1, 47-69 at 48
55 Id. at 68
56 Id. at 49
EXCESSIVE USE OF PRIVACY DESTROYING TECHNOLOGIES AT PUBLIC AND PRIVATE PLACES

Lakhwinder Singh *

*Research Scholar, Department of Laws, Panjab University Chandigarh.

(I) INTRODUCTION

Every soul in the Universe wants to be enlightened. But this can be happened only when the soul lives in an atmosphere, which protects soul’s ‘right to be left alone’. Privacy rights are very important for human beings. Right to privacy proves itself as fundamental to democracy. However, right to privacy is not an absolute claim and, can be restrained on the grounds of public security, peace, public order, and public accountability. Indeed, the government has power of surveillance over its citizens in the interest of the state. And this power of the Government has become more potent with the advancement of the technology. Increasingly, Privacy-destroying technologies like CCTV cameras, biometrics, GPS technology, RFID, DNA or genetic testing, polygraph or other psychological tests, etc., are being used at large scale both by the public and private entities. However, these surveillance techniques are being used in a much unregulated ways.

Therefore, in this research paper, the concept of surveillance has been discussed in detail. Every effort has been made to analyse the use of privacy-destroying technologies in various parts of our society. Furthermore, the research paper includes repercussions of excessive surveillance.

(B) CONCEPT OF ‘SURVEILLANCE’

Whenever, the term ‘surveillance’ comes into our mind, nightmares of Big Brother society start vibrating our thoughts. Basically, the phrase ‘Big Brother is Watching You!’ was used in the novel named ‘1984’, written by George Orwell published in the year 1949. The novel depicts a totalitarian society in which the government has complete surveillance over the people. Big Brother (fictional name given to the government) is supreme ruler and continuously watching people by installing telescreens (giant sized televisions) everywhere in the society like in peoples’ homes, streets, markets, or any other private or public places. The
government does not want people be informed of reality. Every public data is manipulated by
government agencies, as per according to Big Brother’s wish. People are compelled to
believe themselves in an idealist state. The Big Brother’s public policy is

*War is Peace*

*Freedom is Slavery*

*Ignorance is Strength*

And in order to disseminate such type of brainwashing propaganda among people, telescreens
are being used. Furthermore, while spreading government policies in the homes, telescreens
are also capable of recording sounds, images, and facial expressions of individuals and have
enough potential to transmit such material back to the police named, Thought Police. By
recording one’s movement, reflexes, and facial expression, Thought Police easily deciphers
his or her state of mind. By doing so, the police find out what kind of thought he is possessed
with. If thought is against the conservative ideology of Big Brother, then it will be considered
as ‘Thought Crime’. Increasingly, police helicopters frequently snoop in peoples’ windows
and finally, punish ‘thought-criminals’. Therefore, there is no escape from Big Brother’s
camera.

There is no doubt to believe that surveillance controls and regulates human behavior
in every civilized society. But no one expects civilization in the form of ‘Big Brother’
society. On similar lines, it has been established that privacy of man’s home and the security
and integrity of his person and property is not absolute. Law enforcement agencies have the
right to encroach upon rights of privacy and security for compelling reasons. Since
individuals have been struggling from antiquity, balance between state’s interest and
individuals’ privacy interests is needed for healthy civilized society.

The law of privacy is the recognition of the individual’s right to be let alone and to
have his personal space inviolate. The need for privacy and its recognition as a right is a
modern phenomenon. It is the product of an increasingly individualistic society in which the
focus has shifted from society to the individual. In early times, the law afforded protection
only against physical interference with a person or his property. As civilization progressed,
the personal, intellectual and spiritual facets of the human personality gained recognition and
the scope of the law expanded to give protection to these needs.1

The term “surveillance” refers to government efforts to gather information about
people from a distance, usually covertly and without entry into private spaces. Surveillance

---

can be divided into three types. Communications surveillance is the real-time interception of communications. Physical surveillance is the real-time observation of physical activities. Transaction surveillance involves accessing recorded information about communications, activities and other transmissions. Similarly, Alan F. Westin has classified the field of surveillance in three categories i.e. physical surveillance, psychological surveillance and data surveillance.

Governments have long relied on all three types of spying. What is new about today’s surveillance is the ease with which it can be conducted; over the past several decades, technological advances have vastly expanded the government’s monitoring ability.

However, every type of surveillance is not a brand new concept for any society. Eavesdropping and paid surveillance agents go back to antiquity. Torture, sex, alcohol, opium, hypnotism, primitive “lie” tests, and tests for proper “personality” are also ancient ways of unlocking minds, extracting information, or implanting suggestions. As for data surveillance, many societies in the past required registration of residences, movements, and transactions, and used elaborate dossiers and permits as a mechanism of administrative social control. The only shift that took place in the modern world, is the marriage of advanced scientific technology to these classic surveillance methods. While the effort to limit official surveillance over man’s thoughts, speech, private acts, confidential communications, and group participation has for centuries been a central part of the struggle for liberty in the society.

(C) GOVERNMENT’S POWER OF SURVEILLANCE VIS-À-VIS UNREASONABLE SEARCH AND SEIZURE

No doubt, Surveillance is a valuable law enforcement tool but it also poses a significant threat to our legitimate freedoms i.e. privacy and autonomy. In fact since 9/11 attacks in U.S. and 26/11 attacks in Mumbai, the use of privacy destroying technologies have been increased. Even many people justify government’s surveillance power for the sake of their security. In contemporary times, the balance (between privacy and security) shifted toward the security side of the scale. The government has been gathering more information about people and engaging in surveillance. Technology is giving the government unprecedented tools for watching people and amassing information about them-video

---

4 Supra note 2 at 3.
5 Supra note 3.
6 Id. at 67.
7 Supra note 2 at 4.
surveillance, location tracking, data mining, wiretapping, bugging, thermal sensors, spy satellites, X-ray devices, and more. However, the government’s surveillance should be closely watched and subject to meaningful regulation. In U.S. Constitution, there are many provisions which regulate government’s surveillance power. But the constitutional language that most directly speaks to the concerns raised by surveillance is found in the Fourth Amendment, which protects an individual from unreasonable search and seizure.

In United States, telephone wiretapping technology appeared soon after the invention of the telephone in 1876, making the privacy of phone communications a public concern. State legislatures responded by passing laws criminalizing wiretapping. In 1928, in *Olmstead v. United States*, the U.S. Supreme Court held that the Fourth Amendment did not apply to wiretapping because it was not a physical trespass into the home. However, Brandeis gave the dissenting opinion on the point by stating that the new scientific inventions had provided the government such effective means to intrude into one’s home without any physical entry. He also stated 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.

Later on, in *Katz v. United States*, the Court adopted Brandeis’s view, overruling *Olmstead*. In *Katz v. United States* the court held that the government’s action of electronic listening comes within the ambit of “search and seizure” and hence, it is subjected to the Fourth Amendment of the US Constitution.

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. However, it was not until 1965 that the US Supreme Court squarely held that the Constitution contained at least a limited right to privacy.

The US courts have developed privacy right on a constitutional basis. Various amendments of the American Constitution like First, Third, Fourth and Fifth, containing

---

9 Supra note 2 at 4
10 Supra note 8 at 6
11 277 U.S. 438 (1928)
12 Id. at 478
16 M. Glenn Abernathy, *Civil Liberties under the Constitution*, at 95 (1977)
provisions protecting privacy interests has laid the necessary foundation for the courts in this
regard.\(^{17}\)

Recently, in *Kyllo v. United States*\(^ {18}\) the court held that the use of a thermal imaging
device from a public vantage point to monitor the radiation of heat from a person's home was
a "search" within the meaning of the Fourth Amendment, and thus required a warrant.

The earliest case in India to deal with 'privacy' and 'search and seizure' was *M.P.
Sharma v. Satish Chandra*\(^ {19}\) in the context of Art. 19(1)(f) and Art. 20(3) of the Constitution
of India. The contention that search and seizure violated Art. 19(1)(f) was rejected, the Court
holding that a mere search by itself did not affect any right to property, and though seizure
affected it, such effect was only temporary and was a reasonable restriction on the right. The
question whether search warrants for the seizure of documents from the accused were
unconstitutional was not gone into. The Court, after referring to American authorities,
observed that in US, because of the language in the Fourth Amendment, there was a
distinction between legal and illegal searches and seizures and that such a distinction need not
be imported into our Constitution. The Court opined that a search warrant was addressed to
an officer and not to the accused and did not violate Art. 20(3). In the present discussion the
case is of limited help. In fact, the law as to privacy was developed in latter cases by spelling
it out from the right to freedom of speech and expression in Art 19(1)(a) and the right to 'life'
in Art. 21.\(^ {20}\)

Two latter cases decided by the Supreme Court of India where the foundations for the
right were laid, concerned the intrusion into the home by the police under State regulations,
by way of 'domiciliary visits'.\(^ {21}\) Such visits could be conducted any time, night or day, to
keep a tag on persons for finding out suspicious criminal activity, if any, on their part. The
validity of these regulations came under challenge.

In the first one, *Kharak Singh v. State of UP*,\(^ {22}\) the UP Regulations regarding
domiciliary visits were in question and the majority referred to *Munn v. Illinois*\(^ {23}\) and held
that though our Constitution did not refer to the right to privacy expressly, still it can be
traced from the right to 'life' in Art. 21. According to the majority, Clause 236 of the relevant
Regulations in UP, was bad in law; it offended Art. 21 inasmuch as there was no law

\(^{19}\) 1954 SCR 1077
\(^{20}\) *District Registrar & Collector, Hyderabad v. Canara Bank* AIR 2005 SC 186 at 196
\(^{21}\) *Ibid.*
\(^{22}\) 1964(1) SCR 332
\(^{23}\) (1876) 94 US 113
permitting interference by such visits. The majority did not go into the question whether these visits violated the 'right to privacy'. But, Subba Rao J while concurring that the fundamental right to privacy was part of the right to liberty in Art. 21, part of the right to freedom of speech and expression in Art. 19(1)(a), and also of the right to movement in Art. 19(1)(d), held that the Regulations permitting surveillance violated the fundamental right of privacy. In the discussion the learned Judge referred to Wolf v. Colorado\(^{24}\). In effect, all the seven learned Judges held that the 'right to privacy' was part of the right to 'life' in Art. 21.

In the second case, Govind v. State of MP \(^{25}\), in which Mathew, J. developed the law as to privacy from where it was left in Kharak Singh. The learned Judge referred to Griswold v. Connecticut\(^{26}\) where Douglas, J. referred to the theory of penumbras and peripheral rights and had stated that the right to privacy was implied in the right to free speech and could be gathered from the entirety of fundamental rights in the constitutional scheme, for, without it, these rights could not be enjoyed meaningfully. Mathew, J. also referred to Jane Roe v. Henry Wade\(^{27}\) where it was pointed out that though the right to privacy was not specifically referred to in the US Constitution, the right did exist and "roots of that right may be found in the First, Fourth and Fifth Amendments, in the penumbras of the Bill of rights, in the Ninth Amendment, and in the concept of liberty guaranteed by the first section of the Fourteenth Amendment". Mathew, J. stated that, however, the 'right to privacy was not absolute' and that the makers of our Constitution wanted to ensure conditions favourable to the pursuit of happiness as explained in Olmstead v. United States\(^{28}\); the privacy right can be denied only when an 'important countervailing interest is shown to be superior', or where a compelling State interest was shown. Any right to privacy, the learned Judge said, must encompass and protect the personal intimacies of the home, the family, marriage, motherhood, procreation and child bearing. This list was however not exhaustive. He explained that, if there was State intrusion there must be 'a reasonable basis for intrusion'. The right to privacy, in any event, would necessarily have to go through a process of case-by-case development.

In PUCL v. Union of India\(^{29}\), the Supreme Court of India has issued certain guidelines to regulate the practice of phone-tapping like, permission from home ministry is required for every interception, the issuing authority should maintain the complete record of intercepted material, etc.

\(^{24}\) (1948) 338 US 25
\(^{25}\) [1975] 2 SCC 148
\(^{26}\) (1965) 381 US 479
\(^{27}\) (1973) 410 US 113
\(^{28}\) (1927) 277 US 438 (471)
\(^{29}\) AIR 1997 SC 568.
Increasingly, in the case of *Distt. Registrar & Collector, Hyderabad v. Canara Bank* etc., the Supreme Court of India held that right to privacy deals with persons and not places.

Recently in *Selvi v. State of Karnataka*, the Supreme Court held that compulsory administration of any of the techniques, like narcoanalysis, polygraph examination and brain Electrical Activation Profile (BEAP) test, is an unjustified intrusion into the mental privacy of an individual. It was also recognized that forcible intrusion into a person’s mental processes is also an affront to human dignity and liberty, often with grave and long-lasting consequences.

(D) IMPACT OF USA PATRIOT ACT 2001 AND INFORMATION TECHNOLOGY AMENDMENT ACT 2008

In the modern world, an individual’s multi-dimensional relationships with doctors, lawyers, merchants, magazines, employers, credit card companies, insurance companies, phone companies, cable companies, etc., generate records containing personal information necessary to establish an account and record our transactions and preferences. The big problem lies in the fact that such personal information records are held by the third parties. The law enforcement agencies can acquire such information from third party very easily and they don’t even require any kind of lawful warrant.

Eventually, in United States, 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. Eventually, as per according to the Act, the FBI and other agencies can demand that service providers provide access to customer records with a statement certifying that the information pertains to an investigation, without a court order. Mere suspicion of a crime is sufficient cause for law enforcement agencies to conduct wiretap of any telephone number, computer, mobile or email. This is known as ‘roving wiretap’. Furthermore, secret wiretaps are also allowed in the investigation which is being conducted for significant foreign intelligence purpose.

Similarly, in India, under Information Technology Amendment Act 2008, the government can intercept and monitor all communications without any warrant or court order.

---

30 AIR 2005 SC 186.
31 2010(4) SCALE 690
32 Id. at 783
33 Id. at 778
in the security of state or for investigation of any offence. Moreover, India is going to set up a national intelligence grid called NATGRID which will have access to 21 categories of database like railway and air travel, income tax, bank account details, credit card transactions, visa and immigration records. Furthermore, there is every possibility that NATGRID may access the database of Aadhaar cards, which have very personal information including Biometric identification. Therefore, cumulative effects of national population register along with unique identity number, NATGRID and recent Information Technology Amendment Act 2008, have the potential to make Indian Government an Argus State.

Generally, people do believe in the government’s action of surveillance. They consistently participate in every action which seeks their personal information e.g. Census Survey, wiretapping, etc. They have complete trust in the government and, consider such actions as helpful methods in making any public policy. But, after the irresponsible reply by the government, in the case of Ratan Tata, people’s trust has been broken out. The government simply said to the Supreme Court of India that the government could not inquire the leakage of Ratan Tata’s personal information.

(E) VARIOUS TYPES OF PRIVACY DESTROYING TECHNOLOGY

 FrançOIS OR PAT DOWN SEARCH:

It is a search of a person’s outer clothing wherein a person runs his or her hands along the outer garments to detect any concealed weapons or contraband. Eventually, ‘frisking’ is being used at shopping malls, cinemas, multiplexes, streets, Airports, etc. Although the United States has apologized to India for the incident involving the frisking of former President APJ Abdul Kalam at the New York Airport, the incident had led to a huge uproar in India with a debate being raised in Parliament. Other senior Indian officials too have not been spared by US authorities in the past. Indian Ambassador to the United States Meera Shankar, was subjected to a pat down because she was wearing a sari. This was despite the fact that the US authorities were aware of her diplomatic status. And days later India's envoy to the UN Hardeep Puri was subjected to similar checks. But as Kalam is concerned, US authorities had breached protocol when it frisked the former President. Current protocol exempts the President and former Presidents from airport security checks.

---

At shopping malls and multiplexes in India, everyone is subjected to frisking. Although frisking is justified on the ground of security, people feel offended whenever any person touches their bodies. For the time being, people are cooperating with such kind of practice, but, with the increase in sensitivity, and awareness for privacy rights, they will definitely protest against this undignified search.

In the technological era, it is possible to replace pat down search with sophisticated devices. But at the same time, technology, like ‘see through’ technology which have the ability to look under individuals’ clothes, is a serious threat to an individual’s privacy. Indeed, Jeffrey Rosen, Professor at George Washington University, advocates ‘blob machine’ as an alternative to full body scanners. The naked machines reveal not only contraband, metal, or plastics concealed under clothing, but also graphic images of the naked body. There is also an apprehension of stored or recorded images being abused. Hence, naked machine threatens individuals’ privacy. Whereas, in case of ‘blob machines’, only the area of suspicion is revealed, and the screen shows rest of the body as blob-like human image. It is also seen that both types of machines offer identical amounts of security. Therefore, for the sake of privacy protection, public and private agencies should adopt ‘blob machines’ which really preserve privacy.\(^{39}\)

It is submitted that blob machines should be installed as an alternative to frisking at every place. This is to be done irrespective of the fact that whether it is developing nation, Airport, shopping mall, multiplex, or any other place subject to pat down search. It really spreads a sense of dignified life among people who are subject to frisking. Only blob machines can bring the balance between privacy and security.

➢ DNA OR GENETIC TESTING:
Genetic data can serve as an identifier and, as genetic science develops genetic information, which provides a growing amount of information about diseases, traits, and predispositions. In order to increase their productivity and profits, the employers use to conduct genetic tests

on employees for knowing their efficiency, skill or possible diseases in future. Furthermore, DNA samples are being used in the criminal justice system also.\(^4^0\)

Familial DNA testing is a new criminal investigative technique, in which police watch for a close but imperfect match between the DNA left at a crime scene by an unknown offender, and the DNA of a known convicted person in a forensic DNA database. If police find such a match, they may investigate the relatives of the convicted person.\(^4^1\)

In India, DNA Profiling Bill 2007 is pending before Parliament. Once it becomes law, all convicted criminals across the country will have to undergo mandatory DNA tests. The bill will also grant the authority to collect vast amount of sensitive DNA data of citizens even if they are "suspects" in a criminal case.

- **CCTV CAMERAS AND FACIAL RECOGNITION TECHNIQUE:**

CCTV cameras have been installed at every place-public or private. Video recordings are being misused. The camera control operators use such recordings for their own erotic desires or prurient tastes. It has also been revealed that showrooms usually install hidden miniature cameras in the trial rooms.

Moreover, even in public institutions, there is nothing like privacy policy regarding CCTV cameras recordings. Public institutions do not impart any kind of cultural, moral, ethical, technical, and legal education on privacy values to their camera control operators.

- **RADIO FREQUENCY IDENTIFICATION DEVICE:**

Threat of privacy violations, while using Radio Frequency Identification RFID on human beings, has recently been felt by India. In 2011, Indian students at the Tri Valley University, California, had to face virtual imprisonment. This University was shut down after investigators found the University was involved in an immigration fraud. Therefore, after considering them illegal aliens, the Indian students were interrogated by authorities and also forced to wear radio collars fitted with GPS technology to track their movements.\(^4^2\) It was considered as a dehumanizing action on the part of U.S. authorities. It really violates human dignity. Despite such grave violation, RFID technology is being used in most places without any regulations. Such kind of technology is used at the workplaces at very large scale.

\(^4^0\) http://epic.org/privacy/genetic/ accessed on June 6, 2012, at 3:46 p.m IST.
Increasingly, these RFID technologies are also being used in the workplaces to monitor the activities or whereabouts of employees or to gather data on identifiable employees.\textsuperscript{43}

\begin{itemize}
\item \textbf{Psychological Surveillance}
\end{itemize}

Psychological surveillance consists of those scientific and technological methods that seek to extract information from an individual which he does not want to reveal or does not know he is revealing or is led to reveal without a mature awareness of its significance for his privacy.\textsuperscript{44}

Moreover, there are other relations of voyeurism to the problem of surveillance. It was observed by many researchers that polygraph operators do ask embarrassing personal questions to female subjects. It satisfies their erotic desires. Similarly, during wiretapping the authorized officials record the intimate conversation and play it to their friends just for entertainment.\textsuperscript{45}

\section*{(F) IMPLICATIONS OF EXCESSIVE USE OF PRIVACY DESTROYING TECHNOLOGIES}

The degree and nature of privacy accorded to individuals and organizations depends in the first instance on the political system and cultural patterns of the society involved. Totalitarian systems deny most privacy claims of individuals and non-governmental organizations to assure complete dedication to the ideals and programs of the state, while the Totalitarian State’s own governmental operations are conducted in tight secrecy. Democratic societies provide substantial amounts of privacy to allow each person widespread freedom to work, think, and act without surveillance by public or private authorities, and to provide similar breathing room for organizations; but they try to strike a delicate balance between disclosure and privacy in government itself.\textsuperscript{46}

Government information collection interferes with an individual’s freedom of association. Extensive government information gathering from third party records also implicates the right to speak anonymously. There might be an apprehension of being identified, if one speaks against the government’s action. These types of harms can inhibit individuals from associating with particular people and groups and from expressing their views, especially unpopular ones. This kind of inhibition is a central goal of Orwell’s Big

\textsuperscript{44} Alan F. Westin, \textit{Privacy and Freedom}, 133 (1970).
\textsuperscript{45} Id. at 56.
Brother. Although it certainly does not approach the same degree of oppressiveness as Big Brother, it reduces the robustness of dissent and weakens the vitality of our communication.\textsuperscript{47}

Companies and the government are using computers to make important decisions about people based on dossiers, and they are frequently not able to participate in the process.\textsuperscript{48}

Therefore, it is necessary that the government should be required to obtain a special court order when it wants to access personal data that is maintained in a business’s record systems. The law should also allow the people to have greater participation in how the data is used. When public records are made available, the law should do so along with demanding restrictions on access and use.\textsuperscript{49} When the government wants to obtain personal data, the law should mandate that it demonstrate before a neutral judicial official that it has a factual basis that the search will reveal evidence of a particular person’s criminal activity.\textsuperscript{50}

\textsuperscript{47} Supra note 34 at 177.
\textsuperscript{48} Id. at 223
\textsuperscript{49} Id. at 227
\textsuperscript{50} Id. at 228
ROLE OF MEDIA IN DEMOCRACY AND PRIVACY ISSUES

Lakhwinder Singh*

Freedom of speech and expression is the fundamental right of every human being. Such a broad fundamental right also includes freedom of media. It is very essential for every democratic world that its citizens should be well informed. And this responsibility is shouldered on “media” which includes both print and electronic media. The primary duty of the media is to disseminate the news for public well being. At present, with the installation of new technologies, like internet, mobile technologies, etc. the scope of traditional “press”, which included only print media, has become enlarged in the form of electronic media. Consequently, the responsibility of the “media” has also been increased. With the passage of time, the journalists have developed the ideas like sting operations, investigative journalism, etc. to fulfill their responsibility. However, under the protective shield of investigative journalism, the media sometimes over-reaches its power and intrudes the private lives of an individual.

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. The authors criticized the malfunctions of the press. In their view, the press is overstepping in every direction the obvious bound of propriety and of decency. With the commercialization of the press, the Gossip and details of sexual relations became the breaking news. Due to the complexity of life, a man has become more sensitive to publicity and hence, he needs solitude and privacy. But modern enterprise and invention have, through invasions upon his privacy subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

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 freedom of press because the journalists had public regard.¹ This was the time when

*Research Scholar, Department of Laws, Panjab University, Chandigarh
investigative reporting was really doing something for public good. Whereas, today’s media is more concerned about their 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.

The Court’s 1964 landmark decision in *New York Times Co. v. Sullivan* 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. 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.

Further in one of the case the U.S. Supreme Court recognized the society which gives the primary value to freedom of speech and press. The Court held that the freedom of press assures the maintenance of political system and an open society.

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.

Investigative journalism is a kind of journalism in which reporters deeply investigate a topic of interest, often involving crime, political corruption, or some other scandal.

It is necessary for a democratic society that citizens should be well informed. Further, informed citizenry makes the state more accountable and brings the transparency in the whole system. Therefore, investigative journalist shoulders the responsibility to find out the hidden truth which is necessary in the public interest.

---

2 376 U.S. 254 (1964)
3 Id. at 264, 280.
4 Id. at 272, 279–80.
6 Id. at 389
During the 1972 campaign for the White House, when Richard M. Nixon was seeking a second term in office, five persons, acting on orders, broke into the Democratic national offices in the Watergate complex in Washington and planted electronic eavesdropping devices. Their purpose remains unclear till date. Bob Woodward and Carl Bernstein, reporters with the Washington Post, became curious when a short news item appeared regarding a burglary at the Watergate office of the Democratic Party and began to make inquiries. Through investigations it was discovered that it was not a simple act of burglary but a case of political corruption and manipulation involving the highest office in the land.\(^8\)

Reporters are willing to take the responsibility for the truth of their stories, but they use to be reluctant in taking any kind of moral responsibility. Investigative reporters often use various means for their fact-finding like surveillance techniques, miniature cameras, phone records, phone tapping, etc. Many times they even adopt the illegal means to investigate the matter. Obviously, such kind of uses makes the action punishable under the code. For instance, in Tehlaka's Operation Westend case, the undercover journalists used the prostitutes to expose corruption in defence deals.

In the case of Dietmann v. Time Inc.\(^9\) the court held that under the protective shield of freedom of press the journalists have no license to trespass, to steal, or to intrude by electronic means into the precincts of another’s home or office.

In US, after protest by privacy international organization, the judiciary has evolved certain strict guidelines for conducting any kind of Sting Operation like

- String operation could be mounted only against persons against whom some evidence of criminality already exists and a sting operation is considered necessary for getting the conclusive evidence.
- Permission is necessary from court or Attorney-General. This safeguard has been laid down since those who mount a sting operation themselves commit the offences of impersonation, criminal trespass under false pretences and making a person commit an offence.
- There must be a concurrent record in writing of the various stages of the sting operation.

\(^8\) Id. at 16
\(^9\) 449 F.2d 245 (9th Cir. 1971)
• While the transcript of the recordings can be edited, the film and the tapes themselves should not be edited. Where there is evidence of editing, there is an automatic presumption that the recording is probably not authentic.\textsuperscript{10}

On one hand, Sting Operation serves the public interest by strengthening the democratic framework by disseminating information about facts of vital interest to society that are not easy to obtain by simple requests or efforts. The records from the world over show that without the use of SO, public would have never learnt about many economic and political wrong doings. On the other hand, some recent incidents prove the misuse of SO by media and private entities to increase the channel viewership, settle political scores, harm corporate interests, malign reputation etc. Such SO that are carried on with ulterior motives not only harm the person and the institution trapped in the sting, but has the potential to shake people’s faith in the institutions and create a general atmosphere of cynicism in the society.\textsuperscript{11}

The decided case law from Courts on the subject of SO has not laid down any clear cut principles or uniform approach on the legality and extent of permissibility. However certain broad principles are discernible such as the considerations of public interest, the need to recognize the fundamental rights of the targeted persons including the right of privacy and liberty. Also, the illegality inherent in the publication/exhibition of fabricated and misleading content obtained by SO which is universally condemned, is recognized by the courts in India.\textsuperscript{12}

The avowed purpose of the principles of self regulation is stated to be “to empower the profession of Television Journalism by an abiding set of values, which will stand the test of time and ensure that balanced and comprehensive journalism flourishes to strengthen India’s democracy.”\textsuperscript{13}

Invading the privacy of public officials and candidates must be justified by the expected benefits to the public of having information they need as citizens of a democratic society.\textsuperscript{14}

\textsuperscript{10} Supra note 7 at 114
\textsuperscript{11} www.lawcommissionofindia.nic.in/stingoperation.doc accessed on December 4, 2010 at 11.48 p.m
\textsuperscript{12} Ibid.
\textsuperscript{13} Ibid.
In the case of entertainment and sports stars, privacy invasions must be justified by showing that the expected benefits outweigh the potential harms of releasing private information and images of celebrities. The harm to celebrities from invasions of their privacy may include loss of self-determination and self-respect; loss of reputation, status, and revenue; emotional damage; and damage to meaningful relationships. Celebrities’ families may be similarly harmed. 15

Journalists and news organizations earned the profit by offering the audience sensationalized news stories. Simultaneously, the public’s curiosity to know about famous personalities is also being satisfied. Yet, there are certainly many other ways in which the public could be entertained that don’t invade people’s privacy. 16

The information which pertains to entertainment and sports figures does not satisfy the common desires. Rather the potential harms caused by releasing such information are greater than the expected benefits. Such kind of sensational news not only harms celebrities and their families but also destroy the public’s trust in a news outlet. Reputable news organizations would do well to focus attention on the successes and failures of celebrities in their professional fields, rather than delve into their private lives. 17

“Paparazzi” is the term used for freelance news photographers who specialize in candid photos or video of celebrities. Celebrities often complain that paparazzi invade their privacy or endanger them through the use of telephoto lenses and aggressive newsgathering techniques. Paparazzi were initially seen as responsible for the car crash that killed Diana, Princess of Wales, in 1997. That incident, in turn, spawned several attempts in the United States to limit access by photographers to celebrities. 18

Americans were not immune to paparazzi. By the late 1960s, these photographers routinely stalked celebrities in the United States, selling their photos on both sides of the Atlantic. 19

---

15 Id. at 225
16 Ibid.
17 Ibid.
19 Ibid.
In the case of Galella v. Onassis, the court held that disclosing celebrity’s daily habits are not essential for any public’s well being. Therefore, it’s violation of celebrity’s privacy.

Paparazzi encroach upon celebrities’ privacy in two key arenas; public and private. In the United States, the law limits anyone’s privacy rights while that person is in public. When a celebrity—or any person—is in public or in a place where they cannot claim a reasonable expectation of privacy, anyone else generally has the right to photograph them. Because of this legal protection, paparazzi cluster in public places—outside buildings, on sidewalks—where they expect to see celebrities. The paparazzi then follow celebrities, sometimes quite closely and aggressively, for “candid” photos. In most situations, this behavior is legal, if not ethical.

A different legal and ethical issue surrounds photos taken in private settings, usually with the use of telephoto lenses. Celebrities—and others—can generally expect privacy when they are in places not normally seen or frequented by the public, including inside private buildings and on private property, if that property is far from public property. In the United States, it is usually illegal to take photos of individuals in private places, at least if they have taken steps—closing curtains or building fences, for instance—to try to gain privacy. Nevertheless, many paparazzi continue to try to photograph celebrities wherever they are.

Diana, Princess of Wales, was a prime target of paparazzi during and after her marriage to Britain’s Prince Charles. From the time of her marriage to Charles in 1981, celebrity-oriented media followed Diana’s every move. After the couple’s separation and divorce, paparazzi attempted to get photos of Diana with the men she dated. In August 1997 she and her boyfriend, Dodi Fayed, were killed in Paris when their car crashed as their driver attempted to evade paparazzi on motorcycles. Her death brought change in the European Privacy law. The public outcry resulted into the adoption of the European Convention on Human Rights and Fundamental Freedoms in the domestic English Law.

The months following the Princess of Wales’s death saw legislative attempts to curtail paparazzi activity in the United States. In California, one bill would have barred

21 Supra note 18 at 368
22 Ibid.
23 Ibid.
photographers from going within 15 feet of unwilling subjects, and state senator Tom Hayden, the ex-husband of actress Jane Fonda, suggested licensing photographers and creating a “Commission of Inquiry into Paparazzi Behavior.”

In the U.S. House of Representatives, Representative Sonny Bono, himself a celebrity and paparazzi target, introduced the “Protection from Personal Intrusion Act” just 10 days after Princess Diana’s death. This legislation barred “harassing” behavior, defined as following a victim who had a reasonable expectation of privacy, for the purposes of taking a photo, video, or sound recording that would then be sold for profit. The punishment would have been between one and 20 years in prison. The following year, after Bono’s death in a skiing accident, U.S. senators Russ Feingold and Orrin Hatch introduced the “Personal Privacy Protection Act,” which would have outlawed following someone with the intent to take a photo for later commercial gain, when that following caused fear of bodily harm to the subject. While none of these bills at the state or federal level became law, they demonstrated the concern that lawmakers had with paparazzi and invasions of privacy.

Celebrities are entitled to the same general right of privacy that extends to all individuals. However, the degree to which that right is protected is much narrower for public figures. Articles recounting details of the daily lives of celebrities generate a much higher level of interest on the part of the public than do similar stories concerning unknown people. As a result, a broad spectrum of information concerning celebrities is transferred from the protective shield of privacy into the realm of the public interest. The reason behind the narrower degree of protection to the private lives of the public figure lies in certain factors. First, on many occasions, public figures themselves give voluntarily consent to publicity. Second, people’s curiosity makes private affairs of celebrities as “public concern”. Finally, the press has a right to inform the public about matters of public interest.

While the First Amendment of the US Constitution does protect legitimate newsgathering, it does not provide the press with an impenetrable shield from liability for torts committed while gathering the news. Four separate tort actions are available to protect individuals against invasions of privacy by the press: appropriation, false light, public disclosure of private facts, and intrusion.

---

21 Supra note 18 at 369
22 Id. at 290
23 Id. at 293
24 Id. at 293
25 Id. at 290
27 Id. at 290
28 Id. at 293
Contemporary attitudes toward the media and celebrities make it very difficult for celebrities to claim that certain facets of their lives are not newsworthy, especially since celebrities are categorized as voluntary public figures. News and entertainment have been mixed up. So long as the courts and legislature are unwilling to impose standards on the media, the media are left to regulate their own behavior.\(^{29}\)

The public can no longer distinguish between what is and is not news and is becoming disenchanted with techniques that seem to go beyond the realm of public decency. Thus, the legitimate media who serve the true public interest and fulfill their intended role in society must suffer as a result of the actions of their less responsible counterparts.\(^{30}\)

In *Von Hannover v. Germany*,\(^{31}\) paparazzi took pictures of Princess Caroline of Monaco, the eldest daughter of Prince Rainier III of Monaco, which were completely of private nature. Thus, it is important to note that instead of looking to physical zones when determining privacy (i.e., a public or private place), the court determined that certain activities can be exclusively private. The focus is then on the subject matter of the photographs rather than the location where they were taken.\(^{32}\) The court balanced the competing interests of the individual and of the community as a whole. Therefore, the court held that even public figures retain their private interests.

The interests in privacy protected under common law are mainly four in number (basically classified by William Prosser) i.e. Intrusion upon plaintiff’s seclusions or solitude, Public disclosure of embarrassing facts, Publicity which places the plaintiff in false right, Appropriation for defendant’s advantages, of plaintiff’s name and likeness. These interests are regularly protected by English courts with the help of established torts like trespass, nuisance, passing off and defamation.

**CONCLUSION**

More recently, the photograph of Barack Obama, in which it looks like that he casts sly glance at a teenage girl at the G-8 Summit, became very sensitive matter.

In the present era, the media has forgotten its social responsibility and has sold its ethics as well. Under the protective shield of investigative journalism, the media channels are

\(^{29}\) *Id.* at 294

\(^{30}\) *Id.* at 295

\(^{31}\) 2004-VI Eur. Ct. 41

\(^{32}\) *Id.* at 66