CHAPTER - IX
INTERNATIONAL DATA PROTECTION 
AND PRIVACY LAW

9.0 Introduction

Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate world is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information. Moreover, a strong conception of personal data as a commodity is emerging in the United States, and individual Americans are already participating in the commodification of their personal data. Once personal data become a commodity, questions arise regarding the necessity, if any, of legal limits on data trade. Legal scholars interested in protecting information privacy, however, have been suspicious of treating personal data as a form of property and have generally advocated imposing a ban on data trade, rather than restrictions on transferability. In contrast, other legal scholars have advocated propertization of personal information, albeit generally without sufficient sensitivity to privacy concerns. As a result, such scholars usually see no need for legal limits on data trade- that is, no need for "inalienabilities," which, in Susan Rose-Ackerman's succinct definition, are "any restrictions on the transferability, ownership or use of an entitlement."

Since the late 1970s there has been a developing body of international and regional laws and policy instruments relating to the protection of personal data. Most of these instruments articulate broadly similar principles granting individuals specific rights.

over their personal information enforceable against the public and private sectors. These principles are often referred to as Fair Information Practices. They generally require that personal information must be: obtained fairly and lawfully; used only for the original specified purpose; reliable and not excessive to purpose; accurate and up to date; accessible to the subject; and securely stored.

This chapter examines these existing protections for personal data at the international and regional level. Section 1 focuses on the legally binding instruments of the Council of Europe and European Union. Section 2 examines the non-binding, yet influential, measures adopted by the United Nations General Assembly and Organization for Economic Cooperation and Development. Section 3 examines the Privacy law and Data Protection under the Indian Legal system.

The aim of this chapter is to provide a framework for determining what obligations a given country will have under existing international and regional laws to implement and respect the basic principles of data protection.

9.1 Regional Data Protection Treaties

9.1.1 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

In January 1981 the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Convention entered into force in October 1985. It is important to recognize that the Convention is a multilateral treaty as distinct from a statutory act of the Council of Europe. It is therefore legally binding under international law only upon those states that express consent to be bound through the formal act of ratification or accession. As of December 2003, thirty of the Council of Europe's forty-five member states were parties to the Convention and a further five had signed it. The Convention is also open to accession by non-member states of the Council of Europe but so far it has not attracted any non-member parties.

The Convention was the first binding international instrument to protect individuals against abuses in the collection and processing of their personal data. Its purpose is

---

threefold: to introduce basic principles for fair information processing; to establish rules and restrictions on transborder data flows; and to put into place mechanisms for consultation and mutual assistance between the parties.8 It covers automated personal data files and automatic processing of personal data in the public and private sectors.

Chapter II is the core of the Convention, setting out its basic requirements and principles. It begins with an obligation on state parties to “take the necessary measures” to give effect to the basic principles for data protection in domestic law. (Article 4) The term “necessary measures” is not defined and leaves the question of how to give effect to the rules to the discretion of the member states. The Explanatory Report to the Convention explains that apart from legislation, this requirement could also be met by the introduction of regulations or administrative guidelines. It continues that these binding measures could be supplemented by voluntary codes but makes clear that such codes alone would not suffice to comply with the Convention.9 In practice, nearly all state parties have chosen to implement the Convention through legislation.10 The requirement in Article 4 is coupled with an “undertaking” in Article 10 to provide “appropriate sanction and remedies” for violations of data protection principles as implemented into domestic law. Again, the Convention does not specify what constitutes “appropriate” sanctions and remedies. The Explanatory Report lists civil, administrative or criminal measures as possibilities.11

The substantive principles of data protection are set out in Articles 5, 6, 7 and 8. Article 5, provides that all data undergoing automatic processing must be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;

---

10 Id., para. 5.
11 Id., para. 60.
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 introduces the concept of special protection for "sensitive data" which is defined as data revealing racial origin, political opinions, religious or other beliefs, as well as data relating to health, sexual life or criminal convictions. Processing of this data is prohibited in the absence of appropriate legal safeguards. This list is not intended to be exhaustive and may be extended, in accordance with Article 11, to other kinds of data to take into account differing legal and sociological contexts.\(^\text{12}\) Article 7 requires information processors to put into place appropriate security measures to protect against "accidental or unauthorized destruction or accidental loss as well as against unauthorised access, alteration or dissemination." Finally, Article 8 implements the right of individuals to access information concerning them and to demand correction or erasure of this information if it has been processed in a manner inconsistent with the basic principles set out above.

The principles set out in Articles 5, 6 and 8 are not absolute and may be departed from in accordance with one or more of the specific exemptions provided by Article 9. Similar to Article 8(2) of the European Convention, this article provides that derogations of the principles are allowed where they are "provided for by the law of the Party" and "necessary...in a democratic society" in order to protect "State security, public safety, the monetary interests of the State or the suppression of criminal offences" or to protect "the data subject or the rights and freedoms of others." (Article 9(2)) Further restrictions on rights to access provided in Article 8 are allowed "for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects." (Article 9(3))

Chapter III is concerned with the issue of transborder flows of data. It deals primarily with the transfer of personal information between parties to the Convention. It takes as its point of departure the general rule that "a state party shall not, for the sole purpose of the protection of privacy, prohibit, or subject to special authorization transborder flows of personal data to the territory of another party." (Article 12 (2)). However, it permits state parties to derogate from this general rule and to prohibit

\(^{12}\) Ibid., para. 48.
transfers of certain categories of personal data or of automated personal data files which are specifically protected in its national laws and for which the receiving party does not provide “equivalent protection.” (Article 12 (3)(a)). It also permits parties to prohibit transfers to other contracting parties if the data is destined for a non-contracting party in circumvention of the first party’s national law. (Article 12 (3)(b)). This provision is intended to prevent data being “launched” through the intermediary of another state party on its way to a non-contracting state which does not have a satisfactory data protection regime.13 The Convention itself does not deal with the direct transfer of data to non-contracting parties leaving the matter up to the national laws of state parties. This issue is now addressed in the Additional Protocol to the Convention looked at below.

Chapters IV and V put into place mechanisms for implementation and oversight of the Convention. Article 13 requires parties to designate an authority for purposes of co-operation with and assistance to other parties. The Explanatory Report stresses that this Article “does not mean that the Convention requires each state to have a data protection authority. A Contracting State may designate an authority for the purposes of the Convention only.”14 The failure to require national supervisory bodies is also now remedied by the Additional Protocol. Article 14 concerns assistance to data subjects residing abroad who wish to exercise their rights of access under Article 8. It stipulates that data subjects residing in another contracting state are to be given the option of using that country’s designated authority as an intermediary in order to exercise their access rights. Articles 18-20 establish a “Consultative Committee” to be made up of a representative and deputy representative of each contracting party. Non-contracting member states are entitled to observer status on the Committee. Committee is not given any enforcement powers. Its main functions are to propose ways to facilitate or improve the application of the Convention and to make proposals for its amendment. It is to meet at least once every two years or when one-third of the representatives of the parties request it to do so.

13 MITCHELL, supra note 8, at 38.
14 Explanatory Report, CoE Convention, supra note 9, para. 73.
9.1.2 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows 2001

In November 2001, the Council of Europe adopted an Additional Protocol to its 1981 Data Protection Convention. As of December 2003, the Protocol had not yet received the five ratifications necessary in order to bring it into force. The Protocol is intended to close two major shortcomings of the Convention: the failure to address transborder data flows to non-contracting states and the failure to establish national supervisory bodies.

It is a short instrument containing only two substantive provisions. Article 1 requires parties to establish independent supervisory authorities to ensure compliance with the principles of the Convention and the Protocol. These authorities are to be granted the power to receive complaints, to investigate and intervene in cases, to engage in legal proceedings and to refer violations to competent judicial authorities. (Article 1 (2) (a)&(b)) Parties are required to provide a right to appeal decisions of the supervisory authorities through the courts. (Article 1(4)) Supervisory authorities are to “co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging useful information.” (Article 1(5))

According to the Explanatory Report to the Protocol, Article 1 has a dual aim: to enforce the effective protection of the individual; and to improve harmonisation of the rules governing the supervisory authorities already established by parties to the Convention. The Report also clarifies that the powers listed in Article 1 are not intended to be exhaustive and that supervisory authorities may also be entitled to carryout additional duties such as prior checks on processing operations; the maintenance of a public register of data processors; and commentary on proposed legislative, regulatory or administrative measures relating to data processing.

---

16 As of December 2003 only four states, the Czech Republic, Germany, Slovakia and Sweden had ratified the Protocol.
18 Id., para. 16.
Article 2 requires parties to prohibit transfers of personal data to non-contracting states that do not provide an "adequate level of protection for the intended data transfer." Exceptions to this general rule may be provided by law for the "specific interests of the data subject;" or "legitimate prevailing interests, especially important public interests;" or where safeguards are put in place by the controller, for example on the basis of contractual clauses, and these safeguards are deemed adequate by the competent authorities.

The Explanatory Report notes that the "adequacy" of the level of protection must be assessed in light of all the circumstances relating to the transfer including the type of data, the purpose and duration of processing, the country of origin and final destination, and the laws applicable in the state or organization. Furthermore, regard must be had to the principles of Chapter II of the Convention and their implementation in the recipient state or organization. Adequacy can be assessed on a case-by-case basis or for a whole state or organization. At the request of one of the parties, the Consultative Committee may issue an opinion on the level of protection in a state or organization.19

With respect to derogations, the Explanatory Report states that parties must "respect the principle inherent in European law that clauses making exceptions are interpreted restrictively, so that the exception does not become the rule." As examples of "legitimate prevailing interests" it refers to the public interests set out in Article 8(2) of the European Convention on Human Rights and in Article 9(2) of the 1981 Convention; the exercise or defence of a legal claim; or the extraction of data from a public register. As an example of the "specific interests of the data subject" it gives the fulfilment of a contract with, or on behalf of the data subject. It also notes that exceptions may be allowed where the data subject has given his or her consent, provided it is given on the basis of appropriate information.20 Where safeguards are put in place as a result of contractual clauses, the Report stipulates that the content of the contract must include all relevant elements of data protection. Furthermore, it suggests inclusion of procedural terms such as naming a contact person within the staff of the transferring body who

19 Id., paras. 26-30.
20 Id., para. 31.
would be responsible for ensuring compliance and whom the data subject would be free to contact.\footnote{Id., paras 32-33.}

\textbf{9.1.3 Recommendations of the Committee of Ministers}

9.2 European Union Initiatives

9.2.1 EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data 1995

During the 1970s the European Parliament conducted extensive studies in the area of data protection. Concerned that differences in national laws on data protection could result in obstacles to the functioning of a European common market, the Parliament repeatedly recommended the introduction of a directive in this area. The European Commission, however, decided not to take any further action pending the introduction of the Council of Europe Convention. By the 1990s, it was clear that the Convention was not realizing its goal of harmonization of national laws on data protection. Although a number of European countries had introduced data protection laws based on the Convention, there were often considerable differences in the provisions of these laws. Feeling compelled to act; in September 1990 the European Commission issued a draft directive on data protection. Over the next five years, the draft directive was revised and redrafted a number of times as it made its way through each of the different institutions of the European Community. Finally, in 1995 the Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data was approved. The Directive seeks to harmonize national laws within the European Union in order to facilitate the free flow of information across the internal market while simultaneously ensuring a high level of privacy protection for individuals.

The European Directive is the most detailed and complex of the international data protection instruments. Unlike the 1981 Council of Europe Convention which applies only to automated processing of personal data, the Directive applies to "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to

32 See generally MITCHELL supra n. 8, at 31-32.
33 Bennett and Raab, supra note7, at 77.
34 See generally id., at 78-79.
form a part of a filing system."36 However, its scope is limited in two major respects. Although, the Directive generally applies to processing in both the private sectors, it does not apply to the processing of personal data in the course of activities falling outside the scope of Community law. This includes processing concerning public security, defence, State security, and the activities of the State in areas of criminal law. Second, it does not apply to processing by a natural person in the course of "a purely personal or household activity."37

Chapter II sets out the basic principles of fair information processing. It reiterates the principles of the 1981 Council of Europe Convention and extends the protections of that instrument by creating new rights for individuals. Article 6 provides that personal data must be:

1) processed fairly and lawfully;
2) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
3) processed in a way incompatible with those purposes.
4) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
5) accurate and, where necessary, kept up to date, erased or rectified;
6) kept in a form which permits identification of data subjects for no longer than is necessary.

Article 7 further provides that processing may only take place if the data subject has "unambiguously" given consent or if processing is necessary

1) for the performance of a contract to which the data subject is a party
2) for compliance with a legal obligation
3) in order to protect the vital interests of the data subject
4) for the performance of a task carried out in the public interest or in the exercise of official authority
5) for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.

36 1995 EU Directive, Art. 3(1).
37 Id., Arts. 3(2)-(3).
Like the Council of Europe Convention, the Directive provides extra protections for “sensitive” data which is defined in Article 8 as data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Processing of this data is prohibited except where the data subject has given “explicit” consent or where the processing
1) is necessary for carrying out the controller’s obligations in the area of employment law
2) is necessary to protect the vital interests of the data subject
3) is carried out a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim in the course of the legitimate activities and where it relates solely to the members of the body and is not disclosed to a third party
4) relates to data which are manifestly made public by the data subject, or
5) is necessary for the establishment, exercise, or defense of a legal claim.

Articles 10 to 15 create a series of rights to data subjects, beginning with the “right to know” in Articles 10 and 11. These articles stipulate that data subjects are to be provided with information concerning the identity of data controllers; the purposes of the data processing; the recipients of the data; and the existence of a right to access and rectify data. Article 12 sets out the substantive right to access. Under this article data subjects are entitled to obtain “without constraint at reasonable intervals and without excessive delay or cost” confirmation of whether personal data is being processed; details to its intended purpose and use; and information of “the logic involved in any automatic processing of data.” Data subjects are also entitled to the rectification, erasure or blocking of processing of data that is inaccurate or incomplete or processing that otherwise violates the provisions of the Directive (Article 12(b)) Finally, where possible and not involving a disproportionate effort, controllers are to notify third parties to whom data has been disclosed of any such rectification, erasure or blocking of processing. (Article 12(c)) Article 14 grants data subjects the right to object at any time on legitimate grounds to processing being carried out for certain purposes, including direct marketing. Finally, Article 15 establishes the right of individuals not to be subject to decisions made solely on the basis of automated data processing. Provided that suitable safeguards are in place,
exceptions to this right are permitted for decisions taken in the course of entering into or performance of a contract, or for decisions authorized by law.

Articles 16 to 19 concern the duties of data controllers, including the obligation to respect the confidentiality of processing; to ensure a “high level of security appropriate to the risks represented by the processing and the nature of the data;” and to notify the supervisory authority whenever its processing operations are to be wholly or partly automated.

Chapter III of the Directive deals with judicial remedies, liability and sanctions. It requires member states to provide individuals with a judicial remedy for breaches of their rights; to impose liability on data controllers to provide compensation to data subjects for damage caused by unlawful processing; and to put in place suitable sanctions for infringements of the Directive.

Chapter IV concerns transborder flows of personal data. Article 25 sets out as a general rule that data transfers to a “third country” may only take place if that country ensures an “adequate level of protection.” It continues that the question of adequacy is to be assessed “in light of all the circumstances” surrounding the transfer including the nature of the data; the purpose and proposed duration of the processing; the country of origin and final destination; and the laws, professional rules, and security measures in place in the third country. Where the Commission finds that a third country does not ensure an “adequate level of protection,” member states are required to take “all measures necessary” to block transfers to that country. (Article 25(4))

Under Article 26, exceptions to this general rule are permitted when the data subject has given “unambiguous” consent, when the data to be transferred is already contained in a public register, or when the transfer is necessary

1) for the performance of a contract to which the data subject is a party
2) on important public interest grounds or for the establishment, exercise, or defense of legal claims, or
3) in order to protect the vital interests of the data subject

Chapter VI puts in place mechanisms for supervision and enforcement of the Directive. Article 28 requires each member state to establish one or more supervisory authorities to oversee application of the Directive. These authorities must act “in
complete independence" and are to be in entrusted with a large number of powers and responsibilities. For example, they must be consulted during the drafting of administrative measures or regulations concerning data protection. They must also be empowered to monitor, investigate and intervene in data processing activities; to hear complaints; and to initiate legal proceedings. In terms of responsibilities, supervisory authorities are to be required to issue annual reports and to maintain a public register containing information on data controllers operating “wholly or partly automatic” processing systems.

Finally, Articles 29 and 30 establish a Working Party composed of a representative of the supervisory authority of each member state, a representative of the Commission, and representative of other Community institutions. The Working Party is empowered to issue advisory opinions on issues such as the uniform application of national measures to implement the Directive; the level of protection in the Community and in third countries; proposed amendments to the Directive; and codes of conduct drawn up at the Community level. Finally, the Working Party is also entitled to issue recommendations on all matter relating to data protection and is required to issue an annual report regarding the level of protection for personal data within the Community and in third countries.

9.2.2 Directive Concerning the Processing of Personal Data and of Privacy in the Electronic Communications Sector (2002)

In 1997, the European Union supplemented the 1995 directive by introducing the Telecommunications Privacy Directive. The directive sought to translate the data protection principles of the 1995 Directive into specific rules governing the telecommunications sector. The Directive set out obligations on telecommunications carriers and service providers to ensure the privacy and confidentiality of individuals' communications. It prohibited the unlawful interception and surveillance of communications, restricted processing and disclosure of traffic and billing data, and mandated blocking of caller identification technology upon a user’s request. The 1997

---

Directive has now been replaced by the 2002 Electronic Communication Directive, which was introduced to take account new technologies and electronic communications services. It contains new provisions to ensure the protection of all information ("traffic") transmitted across the Internet, prohibit unsolicited commercial marketing by e-mail ("spam") without consent, and protect mobile phone users from precise location tracking and surveillance.

9.2.3 Regulation on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data (2000)

Article 286 of the Treaty Establishing the European Community (as inserted by the Treaty of Amsterdam 1997) provides that as of January 1999 Community acts on the protection of personal data and the free movement of such data shall apply to Community institutions and bodies. Prior to that date, the article required the Council to establish an independent supervisory body to monitor application of these acts to Community institutions and to adopt any other relevant measures.

In December 2000, the European Union issued a Regulation to giving effect to Article 286. The Regulation replicates exactly the central provisions of the data protection directives outlined above. In place of national supervisory authorities, it requires each Community Institutions or body to appoint at least one Data Protection Officer. It also establishes a European supervisory authority known as the European Data Protection Supervisor. The Regulation entered into force in early 2001. The selection process for the European Data Protection Supervisor is still underway.

40 O.J. 2002 C325 (Consolidated Text).
9.2.4 Other Protections

Apart from the data protection directives, there are other provisions in EU law that have a bearing on the protection of privacy and personal data in member states. Article 6(2) of the Treaty on the European Union incorporates the European Convention on Human Rights into "general principles of Community law." As we have seen, Article 8 of the European Convention guarantees a right to "private life" which has been interpreted by the European Court of Human Rights to include protection of personal data.

In addition, the European Charter on Fundamental Rights 2000 includes both a right to private life and personal data. Article 7 provides for respect for "private and family life, home and communications." Article 8 lays down detailed protections for personal data. It provides:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

At present, the Charter simply represents a political declaration, but is intended to form a core part of any future European Constitution. If this is the case, data protection may soon become a fundamental principle of European Community Law directly binding upon member states and enforceable before the courts.

---

42 O.J. 2002 C325 (Consolidated Text).
43 Arts 7 and 8 respectively, Charter of Fundamental Rights of the European Union, December 2000, Official Journal C 364, 18/12/2000)
9.3 Non-binding International Instruments on Data Protection

9.3.1 UN Guidelines Concerning Computerised Data Files 1990

In 1976, the United Nations Secretary General issued a report recommending the drafting of "international standards relating to the protection of the rights of the individual against threats arising from the use of computerized personal data systems", and calling on states that had not already done so to "adopt appropriate legislation containing rules relating to computerized personal data systems in both the public and private sectors."45 This report is recognized as the "parent" in international law of both the Council of Europe Convention and the OECD Guidelines (see below).46

The Secretary General's report also formed the basis of the United Nations Guidelines for the Regulation of Computerized Personal Data Files. These Guidelines were drafted by the Economic and Social Council and adopted, by consensus, by the United Nations General Assembly in December 1990.47 The fact that the Guidelines were adopted by consensus implies that there was no strong opposition to their substance as otherwise a vote would have been required.48 As mentioned earlier in this report, resolutions of the General Assembly do not form binding international law. Nonetheless, they can evidence a general agreement among member states as to what the law is and may acquire a normative status.49

The guidelines set out "minimum guarantees" to be incorporated into national law but leave the question of implementing procedures up to each state. They are intended to apply to all computerized files kept by public and private entities. States are also given the option of extending the guidelines to manual files also (Para. 10). International organizations and non-governmental organizations are covered by the guidelines "subject to any adjustment required to take account of any differences that might exist between files for internal purposes...and files for external purposes." (Sect. B)

46 MITCHELL, at 24.
48 For more on voting procedures of the General Assembly see Philippe Sands & Pierre Klein, Bowett’s Law of International Institutions 266 (2001)
49 Id., at 29.
In terms of substance, the guidelines are very similar to other articulations of Fair Information Practices. They provide for lawful and fair processing (Para. 1); accuracy (Para. 2); purpose-specification (Para. 3); subject access (Para. 4); special protection for sensitive data (Para. 5); adequate security (Para. 7); and limitations on transfer to countries without comparable safeguards (Para. 9). In terms of enforcement, the guidelines call for the establishment of a national supervisory authority, implementation of criminal or other penalties as well as individual remedies (Para. 8).

9.3.2 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data 1980

In 1980 the Organization for Economic Cooperation and Development (OECD) issued important guidelines on privacy and data protection. Although resolutions of the OECD do not form binding international law, they are highly influential and provide clear principles for Member States when developing national policies. Throughout the 1980s, the OECD Guidelines on Privacy Protection, together with the Council of Europe Convention of 1981, were used as a template for the introduction of national legislation in many European countries.

The guidelines set out the following eight principles to be regarded as "minimum standards" for the processing of data by both the private and the public sectors:

a. The Collection Limitation Principle (limiting, and requiring consent, for the collection of personal information)
b. The Data Quality Principle (ensuring the relevance and accuracy of data)
c. The Purpose Specification Principle (requiring the purpose of the information collection to be specified at the time of collection)
d. The Use Limitation Principle (prohibiting use for unrelated purposes except with the consent of the data subject or in accordance with law)
e. The Security Safeguards Principle (requiring reasonable security safeguards to prevent loss, unauthorized access, destruction, modification or disclosure)

---

51 Bennett and Rash, supra note 7, at 75.
f. The Openness Principle (ensuring transparency in the collection process, including the availability of information concerning the data controller)

g. The Individual Participation Principle (providing access for the data subject to his or her personal information and the right to have this data erased, rectified, completed or amended)

h. The Accountability Principle (requiring the effective enforcement of the above principles)52

The guidelines also address the issue of transborder data flows. The general principle is that member countries should refrain from restricting transborder flows of personal data to other member countries "except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation." In addition, member states may impose restrictions on the export of certain categories of personal data which are specifically protected in domestic laws and for which the recipient country provides no "equivalent protection." Where transborder flows do occur, member countries are encouraged to take "all reasonable and appropriate steps" to ensure that such flows are "uninterrupted and secure."53

In October 1998 the OECD adopted a Ministerial Declaration on the Protection of Privacy on Global Networks. In this document member governments pledged to "take the necessary steps...to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks."

9.4 Privacy and Data Protection under Indian Legal System

The word privacy may have different meanings in different perspective in different scenario. Probably this was our culture and living style or the unanticipation about upcoming and fast growing technology that has not compel the lawmakers to include the issue of privacy while framing the legal structure for nation. Before

---

52 Id., paras 7-14.
53 Id., paras 15-18. The provisions on transborder flows must now be read in conjunction with the Declaration on Transborder Data Flows, which was adopted by OECD Ministers in April 1985. The Declaration expresses an intention to "avoid the creation of unjustified barriers to the international exchange of data and information" and to "develop common approaches for dealing with issues related to transborder data flows and, when appropriate develop harmonized solutions."
discussing the e-privacy and data protection in Indian perspective we need to define privacy term.

The word privacy has been derived from the Latin word “Privatus which mean separate from rest”\(^{54}\). It can be define as capability of an individual or group secludes themselves or information about themselves and thereby reveal themselves selectively. Privacy can be understood as a right of an individual to decide who can access the information, when they can access the information, what information they can access.

Indian constitution defines the privacy as personal liberty in Article 21. “Protection of Life and Personal Liberty” No person shall be deprived of his life or personal liberty except according to procedure established by law. The privacy is considered as one of the fundamental rights provided by constitution in list I.

Privacy is recognized at international level as Human Rights\(^{55}\) in different dimension as

a. Privacy of person
b. Privacy of personal behaviour
c. Privacy of personal communication
d. Privacy of personal data.

The word privacy differs from the word confidentiality. We use words privacy, confidentiality and information security synonymously but these words have different meaning and different scope. The word confidentiality simply means Discretion in keeping secret information.

With introduction of various technologies it become difficult to protect the information through confidentiality only and the coverage of protection has been widen to include Integrity and Availability so as to achieve information security. With advancement of latest technology for which many efforts at technological and legal level are done but still there is threat to information because the scope of privacy has been remain still untouched and to provide complete protection to information it is essential to cover the privacy.


\(^{55}\) Privacy And Human Rights http://gilc.org/privacy/survey/intro.html visited 31st January 2013
Although the digitization of data has created convenience in terms of Availability yet it has created havoc of data overflow that leads to difficulty in management of large data, it also includes personal and sensitive information like credit card information. Improper handling of this data can create damage and loss for individual as well Nation. Today business is customer centric and success of any business is depend on users personal preference, in temptation to have technological adaptation, we pass on our personal and sometime sensitive information very easily without giving much concern to privacy. For example from creating a mail account to open an online banking account we pass on our personal information everywhere in day to day life. Ideally the provided information must be used with limited purpose only for which it has been collected but in reality this information is further processed, transmitted and exploited for unauthorized purposes without the permission of data owner56.

In a day we receive almost many unintended calls which offer you various products and services and we never came to know from where this telecaller gets information and details to call us. Actually these calls are resultant of information provided by us unknowingly at some moment of time like when we buy a SIM or opens an account or perform online shopping. Although in given example invasion in privacy lead to disturbance and mental harassment yet some time it may lead financial loss ,damage and even it may cause loss of reputation or life.

This has given primary concern to privacy issue in all over the world in different forms, different countries have adopted various laws and framework to protect privacy not only at legal level but privacy has been endeavoured to protect at technical side. There are many organizations that are working on globally adapted structure of privacy framework like OECD

Based on OECD guideline UK has adopted DPA (Data Protection Act, 1998) which include 8 principles and addresses issues like what is personal information, sensitive information, who is data owner, data subject, who is data processor and who is responsible to protect the privacy.

9.4.1 Legal Challenges

In Indian context there is a lack of proper privacy legislation model so it is extremely difficult to ensure protection of privacy rights. But in absence of specific laws there are some few proxy laws or incident safeguard that the government is using for privacy purpose\textsuperscript{57}.


Lacuna in the present Indian legal frame work for privacy

1) No comprehensive law and still the privacy issue is dealt with some proxy has no convergence on the privacy issue.

2) No classification of Information as public information, private information sensitive information.

3) No legal frame work that talks about ownership of private and sensitive information and data.

4) No certain procedure of creating, processing transmitting and storing the information.

5) Lack of any guideline that defines about Data Quality, Proportionality and Data Transparency.

6) No framework that deals with the issue of cross-country flow of information.

In this era of information technology such loophole in legal framework cannot be ignore and can lead to some severe impairment for individual as well as Nation.

9.4.2 Technological challenges

Globalization and ICT revolution\textsuperscript{58} in India has changes the form of information drastically. It made information more accessible portable and handy. Now day's not only corporate sector but government sector and even individual want to be agile and smart.


\textsuperscript{58} Philip E. Agre, Marc Rotenberg Technology and privacy: the new landscape
Although it has made our life easy, fast and advance but yet it has introduce some unforeseen mayhem and expose our private life.

A list of technologies that have the potential to impact on privacy like Biometrics (such as fingerprints, hand geometry, face, voice, iris and keystroke recognition), Radio frequency identification (RFID), Smart cards, Voice over Internet Protocol (VoIP), Wireless technologies, Location detection technologies (like Global Positioning Systems), Data-matching and data mining technologies, Surveillance Technologies\(^59\).

With the development of Computer Technology, it has not only the ability to store vast amounts of information but also the ability to automatically sort, extract and compare data. Data matching is the process of data mining—looking at certain items of data or at patterns within data as indicators of a particular characteristic, tendency or behaviour. Data-matching poses a particular threat to personal privacy because it involves analyzing information about large numbers of people without prior cause of suspicion. This domain becomes more crucial when data ware houses are managed by third parties like BPO etc.

Security expert Bruce Schneier says, “Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance”.\(^60\)

A number of experts within the field of Internet security and privacy believe that “security doesn't exist;
"Privacy is dead - get over it".

Internet Technologies like cookies, web logger have made the private information more vulnerable.

9.4.3 Current System

Government had started initiative with due care of privacy as it has been discussed above, though India has no codified law to deal with privacy but all the major privacy issue is handled through IPC, ITA Act 2008, Copyright Act, Special relief Act, Telegraph Act, Contract Act, Article 21 and so many other as per of the nature of case.


\(^{60}\) Bruce Schneier The Eternal Value of Privacy, http://www.wired.com/politics/security/commentary/securitymatters/2006/05/7086 visited 31st January 2013
Recently government of India passed special legislation on privacy ITAA 2008\(^{61}\) which give basic definition of Privacy. To implement privacy and data protection in Indian work culture government has established DSCI (Data Security Council of India)\(^{62}\) which was initiative by NASCCOM\(^{63}\). Its mission is to create trustworthiness of Indian company as global sourcing service provider its main aim to create privacy and security awareness among organization. Through awareness and training program DSCI has taken initiative to deal with privacy issue.

Privacy is the most concerned for individual attribute so any case which has been pending in court means mental harassment for user. In India it is necessary to establish fast court system for fast judgment.

In this backdrop, the judgment of the Delhi State Consumer Disputes Redressal Commission (the “Commission”), which imposed a total fine of Rs.75 lakhs on Airtel, the Cellular Operators Association of India (“COAI”), ICICI Bank and American Express Bank on a complaint of consumer harassment by unsolicited telemarketing calls and text messages assumes enormous significance. In 1997, the Supreme Court of India directed the Reserve Bank of India (“RBI”) to institute to implement measures to reduce unsolicited calls on the ground that the right to privacy is a fundamental right.\(^{64}\)

Tort itself falls in the area of discretion. An example of this when Maneka Gandhi moved the Delhi High Court against Khushwant Singh’s autobiography Truth, love and a little malice claiming it had violated her privacy. The judgment went in favour of Khushwant Singh. The two judge bench observed that the right to privacy enshrined in Article 21 could be invoked only against the state action and not against private entities.


As from above case it is clear that Article 21 is to protect privacy of individual against state only.65

Recently India has adopted Right to Information (RTI) which talks about disclosure of public information when it require. It is observed that RTI is an encroachment of Personal information. For successful implementation of RTI it is required to define the Privacy, information classification so that it can help to disclose the information without impairment of routine work.66

IT industries are becoming more concern about privacy. Gist of any IT and ITES industries is information. BPO is major play role in IT industry as there is no legal frame in India about Data Protection.67 They follow third party certification and implement their controls. Mostly in India ISO 27001, Information Security Management System (ISMS) is used to ensure organization due care of all information, which are third party offshore for processing.68

Presently there is no legal architecture for Data Protection Authority, Data Quality and Proportionality, Data Transparency etc.,69 which properly addresses and covers data protection issues in accordance with the principles of the EU Directive, OECD Guidelines or Safe Harbour Principles.70 Accordingly, even if the new proposed amendments to the Information Technology Act, 2000 were adopted, still India is lacking in a real legal framework for Data Protection and Privacy.

67 http://bpo.tcp.in/ Fake it and you break it by: Sunder Ramachandran, visited 31st January 2013
69 Article:"Does India have a Data Protection law"(Mohammed Nyamathulla Khan)http://www .legalserviceindia.com/article/1406-Does-India-have-a-Data-Protection-law.html visited 31st January 2013
Medical tourism or Health tourism in India is an emerging trend. Lots of people from all over the world visit India for their medical, but lack of privacy guidelines of health related record like HIPAA (Health Insurance Portability and Accountability Act)\textsuperscript{73} may have negative impact on this sector.

In India health related privacy issues are dealt with the help of constitution article as in Mr. ‘X’ v. Hospital ‘Z’ for the first time the Supreme Court articulated on sensitive data related to health. In this case, the appellant’s blood test was conducted at the respondent’s hospital and he was found to be HIV (+). Several persons including the members of his family and those belonging to their community came to know of his HIV (+) status and were ostracized by the community. He approached the National Commission against the respondent hospital claiming damages from them for disclosing information about his health, which, by norms of ethics, according to him, ought to have been kept confidential. The National Commission summarily dismissed his complaint. Consequently he moved to Supreme Court by way of an appeal. The Supreme Court observed that as one of the basic human rights, the Right of Privacy was not treated as absolute and was “subject to such action as may be lawfully taken for the prevention and of crime or disorder or protection of health or morals of rights and freedom of others.”\textsuperscript{74}

But still there is no such guideline for health industries to implement health related data privacy protection. Apart from legal framework, there are variety of privacy enhancing technology (PET)\textsuperscript{75} which play vital role for protecting user information PET are the tools application mechanism which are integrated with online application to protect personal information and user identity on the network.

9.5 Framework to protect the Privacy and Personal Data

To observe privacy in Indian work culture we have to adopt above framework which clearly define general guidelines of information addressing in different phases. In

\textsuperscript{73} HIPAA http://privacyruleandresearch.nih.gov/ visited 31st January 2013
this we cover all the necessarily measures while considering the threat to privacy and try to remove vulnerability present in the system. This model mitigates the risk to privacy to the appetite level. So that further threaten to privacy will reduce its impact. The privacy protection is divided in several phases: Data Collection, Data Security, Data Process, and Data Access, e-Govemance, e-Jurisdiction, e-Media, BPO, Telecommunication, Health, e-Business, Tourism, National Security Surveillance, which are described as follows.

1) **Data Collection:**

   First step of privacy protection is start with data collection itself, there must be strict data collection policy impose by the top authority which clearly mention the following points
   
   a) Information is collected by authorize appointed agency only.
   
   b) Information is collected for lawful purpose only.
   
   c) Personal data shall be adequate, relevant and not excessive.
   
   d) Purpose of information collection must be mention.

   If we capture the information properly then it is easy to maintain the information security in next steps. Government shall authorize the agencies for data collection government must also insure that they follow the regulation by doing periodic audit. Whenever information needs for collection it must be collected for lawful purpose only its commercial use is strictly avoided.

2) **Data Security and Storage:**

   After data capture, personal data shall be kept accurately and kept up-to-date. Appropriate technical and organizational measure shall be applied. Technical measures include all information security controls which are necessary to keep information security over internet. If data is store on the server then that server must be fully controlled by government of India. Server must be taken all security safeguard against unauthorized access, use and other modification. Organization measure includes classification of information according to its nature. ‘Segregation of Duties’ and ‘Need to know’ arranges the information according to its need no single person have full control over information user subject is fully mapped with its all information components.
3) Data Process

Personal data shall be processed fairly and lawfully here processing means not only computer processing. We have to process data only when the consent of user is involved, if the user is in contract and one of the party of the contract, process if it's required for judicial proceeding, process if its legitimate use for national interest, process if it's vital interest of data subject. Data should be processed for only given purpose. After processing, the data must be properly disposed. Retention policy must be specified as including purpose and duration of retention.

4) Data Access

The data access must follow Need to Know Basis. There must be control that information not goes beyond the Indian Territory. If data is going beyond territory then appropriate control must be taken to ensure that information is protected outside the India, there must be legal obligation between two countries about data handling. Within the country any Indian or non-government industry process the data it must have to follow all above the norms followed by the Indian government.76

5) e-Governance

There is unique privacy challenges associated with e-governance due to large storage of personal and sensitive data. Obviously e-governance has given new dimension to development and globalization but there should be systematic improvements in governmental privacy leadership; and other technology-specific policy rules limiting, how the government collects and uses personally identifiable information. Government also has unparalleled opportunity to lead by example, by establishing strong, consistent rules that protect citizens without harming the government's ability of functioning. To achieve the specified goal we have to follow certain guidelines77 like:

a) Creating a Union Chief Privacy Officer

b) Installing chief privacy officers (CPOs) at all major departments

c) Ensuring that Data Mining techniques are addressed by the Privacy Act

d) Strengthening and standardizing privacy notices including "privacy impact assessments"

e) Privacy Protection on agency website

f) Complaint processing in case of breach of privacy

6) e-Jurisdiction

Finally India got its first awaited model e-Court at the Ahmedabad City. Evidently the implementation of e-court in India is in its commencing state. The issues like privacy are still untouched. Without substantiation of the standard of technological framework and processes used by e-courts, the system of certainty upon which the courts and law are based has the potential to become inherently uncertain. It will be better to embed the privacy framework to e-court instead of including it later.

The e-court must provide security and privacy of electronic filings. Court shall make any document that is filed electronically publicly available online:

a) There must be unified and coherent policy for the privacy protection and access rights.

b) Except where otherwise noted, the policies apply to both paper and electronic files.

b) The availability of case files at the courthouse will not be affected or limited by these policies.

7) e-Media

E-Media include television channels, radio, internet podcast, and all electronic journalism which are used by today's media. Main purpose of media is to bridge the gap between government policy and public grievances. As there is no information classification in India every information is floated over the media its adverse impact is seen at 26/11 incident all government moves are shown on TV channel which is used by terrorist as a feedback they make their attack strong. Privacy is most concern about celebrities but media is big threat to their privacy every gossip of celebrity is become a Breaking new in most of the new channel. Casting couch is very popular tool used by
media now a day which directly hammer the individual privacy. There is no guideline to handle this issue privacy frame will provide solution to solve this problem.

8) BPO

BPO is Business process outsourcing in IT/ITES industries. BPO play major role for revenue generation in India, complement to BPO there are other types of industries also well establish like KPO (Knowledge process outsourcing), LPO (Legal process outsourcing) and others this is majorly based on information processing. India's BPO industry grew 60 percent to US $6.6 billion in the fiscal year ending 31 March 2008, according to the National Association of Software and Service Companies (NASSCOM)78, in New Delhi. India's business process outsourcing, or BPO, industry says its security standards match the best in the world. There has never been a major instance of data theft in India. Nonetheless, companies in the United States do fear such an event, says Richard M. Rossow director of operations at the U.S.-India Business Council in Washington, D.C. The fear is "not because they are at a higher risk of such a thing taking place in India, but rather because public perception of sending work to India is so bad that it will take only one major event for the affected company to 'pull the plug' on their India data service venture.”79

If we do not ensure companies about strong privacy protection framework, we will lose outsourcing sector. We still rely on some international standard but unless if we not have legal framework, it will difficult to safeguard stake holder interest. Privacy at work place is also ignored field, thousands of workers work in the premises as ‘people are the weakest link in information security’ there must be guideline at work place like cell phone are strictly avoided, prior screening of employee, all work under electronic surveillance, technology used to access employees computer.

78 E-Courts In India http://www.groundreport.com/Opinion/E-Courts-In-India/2912646 visited 31st January 2013
9) Telecommunication

Service providers (SPs) including Internet service providers, number-database operators, telecommunications contractors, emergency call persons; public number directory publishers, authorized researchers and the irrespective employees must protect the confidentiality of information. The use or disclosure of any information or document which comes into their possession in the course of business must be restricted. This could apply, for example, to law enforcement officers who receive billing information, who may receive information in connection with their functions, publishers who receive information in connection with the publication and maintenance of a public number directory, or other service providers who may have received information for billing or network maintenance purposes.

10) Health

Health sector is the important concern in privacy. Your health information includes any information collected about your health or disability, and any information collected in relation to a health service you have received. Many people consider their health information to be highly sensitive. Before proceeding it is very important to consider what all the issues that come under Health Information are:

a) notes of your symptoms or diagnosis and the treatment given to you
b) your specialist reports and test results
c) your appointment and billing details
d) your prescriptions and other pharmaceutical purchases
e) your dental records
f) your genetic information
g) Any other information about your race, sexuality or religion, when collected by a health service provider.

There is certain legislative framework also prepared in other countries for the privacy issue like HIPPA and PSQIA\textsuperscript{80} Patient Safety Rule made by US government. Keeping all this in mind it is mandatory to have a proposed system of health domain that

mainly focused on privacy from Indian perspective. We must have administrative safeguard, technical safeguard, physical safeguard that will clearly define policy and procedure to provide safety of patient information. It covers issues like- there must be supported proceedings in case if someone disclose health information without consent of patient, there must be a written set of policy procedure and designate an officer responsible for implementing the procedure, Policy must clearly define class of employees that are allowed to access Electronic Patient Health Information, access of equipment that contains sensitive information must be properly monitored and controlled, protect your system from direct view of public, before transmitting any information must ensure the authenticity of the other party.

11) e-Business

Indian economy majorly based on e-business outsourcing. We need a privacy framework purely focused on e-business and cover privacy issues and provide legal assistance in case of any fraud, crime. Issues that are need to cover under privacy framework like proper storage of sensitive credentials like credit card, safe credit of money during online transaction, Confidentiality, Integrity availability, authentication of party must be ensured before beginning of transaction, Encrypt the data before transmission of sensitive information, Restrict access based on need to know basis, assign unique identification to the parties that are involved in the business for authentication purpose. Also maintain the policy that addresses e-business privacy.  

12) Tourism

India is the vast combination of heritage and culture. Due to this reason it generates most of the revenue 6.23% to the national GDP and 8.78% of the total employment in India from the tourism industry. When tourist visits in India they perform several transaction, but there is no guarantee that this provided information is not further misused.

Each tourist must have right that their information is protected, corrected, erased as per their wish. Employing the most appropriate physical and technical measures, staff training and awareness, to ensure that unauthorized access to, alteration or destruction of personal data does not take place. Similarly for the Medical Tourism the personal information of the patient must be protected. After the completion of the transaction the credit card information must be destroyed.83

If such issues are covered in the privacy framework of the tourism then it must add on in Indian revenue, tourist feel safe while visiting the country, it also reduce the crime rate.

13) National Security Surveillance

The collection of personal information by means of a surveillance system is lawful and justifiable as a policy choice, and if so, it must be ensured how privacy protective measures can be built into the system. "Reasonable expectation of privacy" is one of the keys to surveillance being legal.84

Using surveillance systems to address concrete, confirmed problems and/or incidents is acceptable only if the practice meets all statutory requirements. The activities like Access, Use, Disclosure, Retention, Security and Disposal of Surveillance Records must be regulated.85

a) Prior to adopting a proposed surveillance program/practice an assessment of the impact on privacy is necessary
b) Public bodies should consider public consultations prior to introducing surveillance and inform those impacted once adopted
c) The design and operation of surveillance program/practice should minimize privacy intrusion to what is absolutely necessary to achieve its goals like designing and installing Surveillance Equipment
d) System operators require privacy-sensitivity training

---

For National Security purpose this definition assumes to be optimism. It’s a matter of preserving national security, heritage, culture and life of each citizen. When we talk about national security with privacy concern then it is more focused on the safeguard of country sensitive information, agreement and security policies. Privacy of national security can be breached when espionage like activity can be performed by an individual to harm the reputation of the country.  

With respect to national security there is exemption of privacy from it. Must have separate framework with proper defined national security privacy guidelines. It must include that the government has authority to investigate about any citizen, can seize any personal information regarding an individual when it mounts to National Security, because it is primary and foremost concern. Authority can access information anytime whether it belongs to private and public interest if they found susceptible or threat to national security. It has overall authority as it is deal with the preservation of millions of life.

### 9.6 Conclusion

With increasing value and importance being attached to personal data by companies throughout the world, it is becoming increasingly urgent that effective protection is afforded to it. It is increasingly unacceptable that an issue of such importance is squeezed into existing, ill-fitting laws. Current data protection laws date from the pre-Internet era and although the Directive makes a valiant attempt to protect such privacy, it simply was not designed to cope with the sheer scale of the problem it now faces. Meanwhile, existing privacy laws, such as they are, in the UK are unreliable for this task, with the discussion above demonstrating the continuing uncertainty as to what exactly the law in this area is. It is thus necessary to seek a new solution, not based upon existing laws, that stems from a respected and authoritative multi-national body. The most notable omission from the discussion above is any suggestion of the type and degree of protection any tailor made online data privacy regulation would offer. This is perhaps due to the size of the task and in part due to the fact that this chapter hoped to

---

provoke some debate as to the suitability of a European Regulation as a possible solution to the current data privacy problem. It is nevertheless an issue I would hope to return to. Seeking to protect online data privacy through means of a regulation in the now twenty-five member EU, it is contended, would be a positive step forward. It will be by no means an ideal solution although as the power and size of the Internet continues to grow, it is increasingly important that the law begins to think ‘outside the box’ if we are not to be drowned by a tidal wave that would make the ‘tide’ of Community law that Lord Denning complained of appear as no more than a ripple on the transatlantic pond in comparison.