**PRIVACY AND DATA PROTECTION IN CYBERSPACE**

**IN INDIAN ENVIRONMENT**

BY

**Bijan Ghosh**

INTERN

10th Semester,

Department of Law,

North Bengal University

Mob- 7001682141

Email- bijanghosh015slg@gmail.com



www.probono-india.in

**May 15, 2020**

**Privacy and Data Protection in Cyberspace**

**in Indian Environment**

***“You can have security and not have privacy, but you cannot have Privacy without security.”***

*—Tim Mather*

**Abstract :**

This paper deals with the privacy issue, concerning challenges in three various aspects like Legal, Technical and Political domain in Indian perspective. This paper suggested framework to deal with these challenges. Growth in technology such as Mobility, Data Mining, Cloud computing etc. brings unexpected challenges and one of the major challenges is threat to “privacy”. Presently we can obtain any information related to anyone from anywhere at any time but this arise a new problem to private and confidential information. Globalization has given acceptance of technology in the whole world, asper demand increases different countries has established different legal framework like Data Protection Act of 1998,UK;Electronic Communications Privacy Act of 1986, USA etc. from time to time ,but in India there is no such inclusive legal framework that deals with privacy issue. To handle vital cyber challenges we refer IT Act 2008 that was set up with the motivation to facilitate e-commerce and hence the privacy was not advance concern in IT act. This suggestive framework give inclusive solution as per present and future requirements of privacy in Indian scenario. As rightly said “true power of any law lies on its ability and ease of enforcement”.

**Key words:** privacy; legal framework; globalization; technology

**Introduction:**

The word privacy may have various meanings in various perspective in various scenario. Most probably this wasour culture and living style or the expectation about upcoming and expand technology that has not forcethe lawmakers to incorporate the issue of privacy while making the legal structure for nation. Before we talk about the e-privacy and data protection in Indian perspective we need to define privacy term.

The word privacy has been derived from Latin word “Privatus” which mean “different from rest”. It can be define as ability of an individual or group separate themselves or information about themselves and thereby disclose themselves selectively.[[1]](#footnote-2)The word privacy can be described as a right of an individual to decide who can acquire the information, when they can acquire the information and what information they can access. Indian constitution defines the privacy as personal liberty under Article 21. “Protection Of Life And Personal Liberty” No person shall be deprived of his life or personal liberty except according to procedure established bylaw. The privacy is considered as one of the fundamental rights provided by list I of constitution.

Privacy is recognized at international level as Human Right in different dimension as

* Privacy of person
* Privacy of personal data
* Privacy of personal behavior
* Privacy of personal communication.

The word privacy means confidentiality. We use words privacy, confidentiality and information securitysynonymously, but these words have different meaning and different scope. The word confidentiality simply means Discretion in keeping secret information.

Present day, with introduction of different technologies it become tough to protect the information through secretly only and the analysis of protection has been broadened to include Integrity and Accessibilityso as toachieve information security. With improvement of latest technology for which many efforts at technological and legal level are done but still there is warning to information because the extent of privacy has been remain untouched and to provide absolute protection to information it is essential to cover the privacy. Although the digitization of data has generated convenience in terms of Accessibility, yet it has created damageof data overflow that leads to difficulty in management of large data, it also includes personal and sensitive information like credit card information. Inappropriate handling of this data can create damage and loss for individual as well Nation.

Present-day business is customer centric and success of any business is depending on taste of users, in temptation to have technological adaptation, we pass on our personal and sometimedelicate information very easily without giving great concern to privacy.

There are many organizations that are working on globally adapted structure of privacy framework like OECD. Based on OECD guideline UK has adopted Data Protection Act, 1998 which include 8principles 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.

**II. Legal Challenges:**

In context of India, there is anabsence of genuine privacy legislation model so it is extremely difficult to ensure protection of privacy rights, but in absence of specific laws there are some few substitute laws or incident safeguard that the government is using for privacy purpose.

Particular legislative framework that provides indirect support to privacy concerns in India, like Article 21, Indian Constitution; IT Act 2000; Indian Telegraph Act, 1885;The Indian Post Office Act, 1898; Code of Criminal Procedure, 1973; The Indian Wireless Telegraphy Act, 1933; Central Motor Vehicles Act 1898 and 2012.

**The Constitution**

The Indian Constitution guarantees a fundamental right to privacy. This was upheld before the Supreme Court in August 2017. This case was brought to the Supreme Court after the claim in the 2015 by Mukul Rohatgi, the then Attorney General stated that there is no constitutionally guaranteed right to privacy. This claim was denied by the nine-judge bench of the court, which found that the constitution does guarantee a right to privacy. Importantly, the case strikes down M.P Sharma and Kharak Singh, to the extent that the 2017 judgement holds that Indian Constitution does uphold a right to privacy.

In the judgment of the Supreme Court, the right to privacy has been read into two articles of the constitution: Article 21, and Part IIIof the Constitution. This means that any limitation on the right in the form of reasonable restrictions must not only satisfy the tests evolved under Article 21, but where loss of privacy leads to infringement on other rights, such as chilling effects of surveillance on free speech, a constitutional framework now exists for these cases to be heard within.[[2]](#footnote-3)

The Supreme Court Judgement also upholds the decisions made after Kharak Singh on privacy, subject to the above conditions. Thus, it is important to understand the contours of the right to privacy and its restrictions in India from the other case law that exists:

* The right to privacy can be restricted by procedure established by law and this procedure would have to be just, fair and reasonable (Maneka Gandhi v. Union of India);
* Reasonable restrictions can be imposed on the right to privacy in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence; (Article 19(2) of the Constitution of India, 1950)
* The right to privacy can be restricted if there is an important countervailing interest which is superior to it (Govind v. State of M.P.);
* The right to privacy can be restricted if there is a compelling state interest to be served (Govind v. State of M.P.);
* The protection available under the right to privacy may not be available to a person who voluntarily introduces him- or herself into controversy (R. Adijagopal v. Union of India).

**Case Law**

There are a large number of cases where Indian Courts have recognised the right to privacy as a fundamental right. Below is a list of landmark cases that have elaborated on the right to privacy along with short points on what the Court has held in those cases:

***Kharak Singh v. The State of U.P. (1962AIR 1295)[[3]](#footnote-4)****,* in this case before the Supreme Court, a minority opinion recognized the right to privacy as a fundamental right. The minority judges located the right to privacy under both the right to personal liberty as well as freedom of movement.

***People’s Union for Civil Liberties v. Union of India (1996SC 568)[[4]](#footnote-5)****,* this case before the Supreme Court extended the right to privacy to communications. In doing so, the Court laid down guidelines that form the backbone for the checks and balances in interception provisions in India such as:

(i) Interception orders to be issued only by Home Secretaries at both the Central and State governments.

(ii) Issues such as the necessity of the information and whether it can be acquired by other means to be considered while making the decision to approve interception.

(iii) The addresses and the persons whose communication has to be intercepted should be specified in the order, which means that the interception order cannot be generic; and

(iv) Putting a cap of two months on the life of an interception order.

***Selvi and others v. State of Karnataka and others (AIR 2010 SC 1974)[[5]](#footnote-6)*** The Supreme Court acknowledged the distinction between bodily/physical privacy and mental privacy. The scheme of criminal and evidence law mandates interference with the right to physical and bodily privacy in certain circumstances, but the same cannot be used to compel a person "to impart personal knowledge about a relevant fact". This case also establishes the intersection of the right to privacy with Article 20(3) (self-incrimination). An individual's decision to make a statement is the product of a private choice and there should be no scope for any other individual to interfere with such autonomy. Subjecting a person to techniques such as narcoanalysis, polygraph examination and the Brain Electrical Activation Profile test without his or her consent violates the subject’s mental privacy.

***Justice K.S. Puttuswamy (Retd.) &Anr. v. Union of India &Ors. (WRIT PETITION (CIVIL) NO 494 OF 2012)[[6]](#footnote-7)***In this Supreme Court order, the issue of privacy was discussed in light of the Unique Identity Scheme. The question before the court was whether such a right is guaranteed under the Constitution, and if it is, the source of this right, given that there is no express provision for privacy in Indian Law. The Attorney General of India argued that privacy is not a fundamental right guaranteed to Indian citizens. Ultimately, the Court left the question to be deliberated by a larger constitutional basis since the earlier judgments that denied the existence of the right to privacy were given by larger benches than the cases where the right to privacy was accepted as a fundamental right. This led to unresolved controversy, leading the Court to refer the matter to a larger bench to be settled. This was settled in the 2017 ruling that there was a fundamental right to privacy in the constitution.

**Information Technology Act 2008 and Telegraph Act, 1885**

There are two major laws that regulate digital and telephonic surveillance, respectively: the **Information Technology Act2008** (the IT Act) and the **Telegraph Act, 1885** (the Telegraph Act).

Section 5 of the Telegraph Act empowers the Central Government and the State Government to order the interception of messages in two circumstances:

(1) in the occurrence of any “public emergency” or in the interest of “public safety”, and

(2) if it is considered necessary or expedient to do so, in addition to the following instances: in the interests of the sovereignty and integrity of India; the security of the State; friendly relations with foreign states; public order; and for the prevention of incitement to the commission of an offense.

In 2007, Rule 419A was added to the Indian Telegraph Rules (1951) framed under the Indian Telegraph Act. These Rules provide that orders for the interception of communications must be issued by the Secretary in the Ministry of Home Affairs in the case of the Central Government and the Secretary to the State Government in-charge of the Home Department in the case of a State Government. However, the Rules provide that in unavoidable circumstances an order can also be issued by an officer, not below the rank of a Joint Secretary to the Government of India, who has been authorized by the Union Home Secretary or the State Home Secretary.

The IT Act widely regulates the interception, monitoring, decryption and collection of information of digital communications in India. More specifically, section 69 of the IT Act empowers the Central Government and the State Governments to issue directives for the monitoring, interception or decryption of any information transmitted, received or stored through a computer resource. Section 69 of the IT Act expands the grounds upon which interception can take place as compared to the Telegraph Act. As such, the interception of communications under Section 69 is carried out in the interest of: the sovereignty or integrity of India; the defense of India; the security of the State; friendly relations with foreign States; public order; the prevention of incitement to the commission of any cognizable offense relating to the above; and for the investigation of any offense.

Although the grounds for interception are roughly the same as under the Telegraph Act, the IT Act does not contain the overarching condition that interception can only occur in the case of public emergency or in the interest of public safety. Additionally, section 69 of the IT Act mandates that any person or intermediary who fails to assist the specified agency with the interception, monitoring, decryption or provision of information stored in a computer resource shall be punished with an imprisonment for a term which may extend to seven years, and shall be liable for a fine.[[7]](#footnote-8)

Section 69B permits authorized authorities to monitor and collect traffic data for the purpose of enhancing cybersecurity and for the identification, analysis and prevention of any intrusion or spread of computer contaminant in the country. A service provider that fails to comply with the provision faces imprisonment up to three years and is liable for a fine. The term “cyber security” has been defined in section 2(nb) of the IT Act as “protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction”[[8]](#footnote-9). Further clarity on the meaning and importance of the term can be gleaned from the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 which are discussed below.

The main difference between Section 69B and Section 69 is that while the latter requires the interception, monitoring and decryption of information generated, transmitted, received or stored through a computer resource, Section 69B specifically provides a mechanism for all metadata through a computer resource for the purpose of combating threats to “cyber security”. Directions under Section 69 can be issued by the Secretary to the Ministry of Home Affairs, whereas directions under Section 69B can be issued by the Secretary of the Department of Information Technology under the Union Ministry of Communications and Information Technology.

Just like with Rule 419A of the Indian Telegraph Rules, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (“IT Interception Rules”) are framed under Section 69 and the Information Technology (Procedure and Safeguards for Monitoring and Collecting traffic data or information) 2009. These stipulate who may issue directions for interception and monitoring; how such directions are to be executed; the duration they remain in operation; to whom data may be disclosed; the confidentiality obligations of intermediaries; periodic oversight of interception directions by a Review Committee under the Telegraph Act; the retention of records of interception by intermediaries; and the mandatory destruction of information in appropriate cases.

Apart from the above two statues, a number of criminal statutes provide for the interception of communications and how such intercepted communications may be used. The Unlawful Activities Prevention Act, 1967 allows for information collected through interception of communications to be produced as evidence for an offence under the Act.

However, intercepted communications are not admissible unless the accused is given a copy of the order approving the interception, thus making illegal interceptions inadmissible. Therefore, unless the interception order itself was obtained by fraud, this provision acts as a safeguard against the use of illegally obtained interceptions for evidentiary purposes. Apart from this Act there are a number of pieces of state legislation that provide for the interception of communications, including the Maharashtra Control of Organized Crimes Act, 1999 and the Andhra Pradesh Control of Organised Crime Act, 2001 .

**The Indian Post Office Act, 1898**

Section 26 of the Indian Post Office Act, 1898 empowers the Central Government and the State Governments of India to intercept postal articles. In particular, section 26 of the Act states that: on the occurrence of any public emergency or in the interest of public safety or tranquility, the Central Government, State Government or any officer specially authorized by the Central or State Government may direct the interception, detention or disposal of any postal article, class or description of postal articles in the course of transmission by post. Furthermore, section 26 states that if any doubt arises regarding the existence of public emergency, public safety or tranquility then a certificate to that effect by the Central Government or a State Government would be considered conclusive proof of such a condition being satisfied.[[9]](#footnote-10)

**Code of Criminal Procedure, 1973**

Section 91 of the Code of Criminal Procedure, 1973 regulates targeted access to stored content. In particular, section 91 states that a Court in India or any officer in charge of a police station may summon a person to produce any document or any other "thing" that is necessary for the purposes of any investigation, inquiry, trial or other proceeding under the Code of Criminal Procedure. Under section 91, law enforcement agencies in India can access stored data. If the Commissioner of Police or Superintendent of Police believes that such a document, parcel or thing is required for the above-mentioned purposes, he may require the postal or telegraph authority to detain such item pending an order from a court. Section 92 of the Code also allows District Magistrates and Courts to issue directions requiring document, parcel or “things” within the custody of any postal or telegraph authority to be produced before it if needed for the purpose of any investigation, inquiry, trial or other proceeding under the Code.[[10]](#footnote-11)There is little judicial clarity on the subject but it has been argued that it is possible to interpret the provisions in a way that even private ISPs can be considered as postal or telegraph authorities and thus become subject to interception under this section. The level of protection granted to postal or telegraph authorities under section 92 is higher than that provided to ordinary citizens under section 91 since even a police officer in charge of a police station can ask for items to be produced whereas under section 92 it has to be either the District Magistrate or a specified Court.

**The Indian Wireless Telegraphy Act, 1933**

Under section 3 of the Indian Wireless Telegraphy Act, 1933, the possession of wireless telegraphy apparatus without a license is considered an offense. As such, the unauthorized establishment, maintenance or operation of wireless communications networks for the purpose of monitoring, intercepting and surveilling communications is in violation of the Act.[[11]](#footnote-12)

**Central Motor Vehicles Act 1898 and 2012 Rules**

In October 2012, Rule 138A of the Central Motor Vehicle Rules, 1989 concerning radio frequency identification tags, was proposed.[[12]](#footnote-13) This proposed Rule mandates the installation of radio frequency identification (“RFID”) tags on all light and heavy motor vehicles to enable their instant identification and monitoring by electronic collection toll booths, the police and any other authority or person that is able to query and read RFID tags.

**Data retention**

Data retention standards can be found in the operating licenses and in the Information Technology Act, 2000. According to the operating licenses, service providers are required to maintain all commercial records for one year. This includes the called and calling party, their locations, the telephone numbers of call forwarding, data records of failed call attempts, and call data records. Under section 3(4) of the Information Technology Intermediary Guidelines Rules, intermediaries are required to retain content that has been removed and associated information for a period of 90 days. Under section 4(2) of the Information Technology Guidelines for Cyber Cafes Rules, cyber cafes are required to retain copies of user identification for a period of one year. Section 5 of the Rules requires cyber cafes to retain logs of user information and browsing history for a period of one year.[[13]](#footnote-14)

**Remedy**

To date, there is no statutory redress mechanism that an individual can resort to in cases of suspected illegal interception. The most that an individual can do is to approach the court and claim an invasion of his/her right to privacy. In such a case, the redress available would be determined by the Court itself. A number of statutes penalize unlawful surveillance. For example, Section 24 of the Indian Telegraph Act states that the penalty for unlawful interception is a fine of up to 500 rupees and imprisonment of up to one year. In case of unlawful interception by a telegraph officer or person with official duties connected to a telegraph office, the penalty is a fine or imprisonment of up to three years or both. The Rules under section 69 of the Information Technology Act, 2000 provide that service providers or their employees who intentionally and without authorization attempt to intercept, authorize, or assist any person to intercept information in transmission at any place within India will be punished according to the relevant provisions. In case of unauthorized interception by security agencies, no specific penalty is provided for but there is a “catch-all” penalty under the ITA (section 45) that states that any person who contravenes any provisions of the ITA or the Rules or Regulations under the ITA would be liable to pay a fine not exceeding 25,000 rupees.[[14]](#footnote-15)

**Case law**

Case law dealing with surveillance has been extremely influential in shaping the privacy landscape in India. The major case on surveillance are given below:

*N.C.T. of Delhi v. Navjot Sandhu* in this case, the Supreme Court held that the pre-requisite conditions under a special statute such as the Prevention of Terrorism Act for admitting the evidence collected against the accused through the interception of wire, electronic or oral communication have to be complied with before accepting such material as evidence.

It therefore appears that under Indian law, if the statute under which a person is being charged is silent as to the admissibility of illegally obtained evidence, then such evidence may be accepted in court. However, it is up to the Judge to decide how much reliance, if any, is to be placed on such evidence. However if the statute in question has a specific procedure by which such evidence has to be collected, then such evidence will not be admitted if the procedure has not been complied with.

**Regional and international conventions**

India is party to two international instruments containing privacy protections. These are the Universal Declaration on Human Rights (Article 12) and the International Convention on Civil and Political Rights (Article 17).

**There is following lacuna in present Indian legal frame work for privacy**

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

 No classification of Information as public information, private information sensitive information.

 No legal framework that talks about ownership of private and sensitive information and data

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

 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.

**III. Technological challenges:**

Globalization and ICT revolution 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. Although it has made our life easy, fast and advance but yet it hasintroduce 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, Smartcards, Voice over Internet Protocol, Wireless technologies, Location detection technologies (like Global Positioning Systems),Data-matching and data mining technologies, Surveillance Technologies.

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 characteristic, tendency or behavior. 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”.

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 has made the private information more vulnerable.

**Apolitical and Social Challenges:**

Any technology needs strong support of human resource for its successful implementation. In political challenges we talk about people factor who are stakeholder for a given technology. Information Technology principle says that people are the weakest link in Information Security.

In Indian scenario people play vital role, people are the policy maker who will decide and direct the path for any technology. Though the Privacy issue is not at pinnacle in our culture because people are least bother about their privacy and there is no scam till now that directly impact on privacy but it is well said that prevention is better than cure.

The major offshore work of BPO is from that country who have implemented legislative framework in the form of codified law like all Europeans countries follow DPA 1998, United State follow ECPA. They do business in India just because investment cost is very low. They due care of their data with compliance of someone-government international organization like ISO, ITIL and other.

Most of cases are pending in family court because of the breach of privacy on the ground of violation of trust between two parties.

Media play an important role in democracy to make people aware about information related to government policy and what the grievances people have but now a day media encroaches on public life, no one’s personal information is kept secure for their own interest.

India has adopted new technologies, there is new trend of connecting people using social networking sites like Orkut, Facebook etc., and here we find people of same interest group together called as community. In such communities lots of people share the information of latest happening, they express their views, criticize on certain issue. All these activities can elevate sensitive issue, which may lead to communicable, misbalanced in the society. Blogs are increasingly popular in today’s world. Writing blogs, people can express their thought and their views but in public and government sector, So there is possibility that private information may be forged and its original intension may be lost.

**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, ITAct2008,Copyright act, Special relief Act, Telegraph Act, Contract Act, Article 21 and so many other as per of the nature of case. Recently government of India passed special legislation on privacy ITA 2008 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) which was initiative by NASCCOM. Its mission is to create trustworthiness of Indian company as global sourcing service provide 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, which imposed a total fine of Rs.75 lakhs on Airtel, the Cellular Operators Association of India, 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 to institute to implement measures to reduce unsolicited calls on the ground that the right to privacy is a fundamental right.

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 favor 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.

Recently India has adopted Right to Information (RTI) which talks about disclosure of public information when itrequire. 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.

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.

They follow third party certification and implement their controls. Mostly in India ISO 27001, Information Security Management System is used to ensure organization due care of all information, which is third party offshore for processing.

Presently there is no legal architecture for Data Protection Authority, Data Quality and Proportionality, Data Transparency etc. which properly addresses and covers data protection issues in accordance with the principles of the EU Directive, OECD Guidelines or Safe Harbor Principle. 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.

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 Health Insurance Portability and Accountability Act may have negative impact on this sector.

**VI. Proposed Framework:**

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 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. We divide the privacy protection in four phases Data Collection, Data Security, Data Process, and Data Access which describe are as follows.

**(a)Data Collection**

First step of privacy protection is start with data collection itself, there must be strict data collection policy imposed by the top authority which clearly mention the following points

 Information is collected by authorize appointed agency only.

 Information is collected for lawful purpose only.

 Personal data shall be adequate, relevant and not excessive.

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 ensure 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.

**(b)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.

**(c) Data Process**

Personal data shall be process 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 process for only given purpose. After processing, the data must be properly disposed. Retention policy must be specified as including purpose and duration of retention.

**(d) Data Access**

The data access must follow Need to Know Basis. There must be control that information does not go 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 they must have to follow all above the norms followed by the Indian government.

**VII. Findings:**

**(a) 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 guidelines, like:

 Creating a Union Chief Privacy Officer

 Installing chief privacy officers at all major departments

 Ensuring that Data Mining techniques are addressed by the Privacy Act

 Privacy Protection on agency website

 Complaint processing in case of breach of privacy

**(b) 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 frame work 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.

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

 Except where otherwise noted, the policies apply to both paper and electronic file.

**(c) 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.

**(d) 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, 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.”

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 do not have legal framework, it will difficult to safeguard stake holder interest. Privacy at work place is also ignored field, thousands of workers are 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.

**(e)Telecommunication:**

Service providers including Internet service providers, number-database operators, telecommunications contractors, emergency call persons; public number directory publishers, authorized researchers and their respective 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 inconnection 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.

**(f) 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:

 notes of your symptoms or diagnosis and the treatment given to you

 your specialist reports and test results

 your appointment and billing details

 your prescriptions and other pharmaceutical purchases

 your genetic information

 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 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 a 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.

**(g) 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.

**(h)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. Using surveillance systems to address concrete, confirmed problems and/or incidents is acceptable only if the practice meets all statutory requirements.[[15]](#footnote-16) The activities like Access, Use, Disclosure, Retention, Security and Disposal of Surveillance Records must be regulated

 Prior to adopting a proposed surveillance program/practice an assessment of the impact on privacy is necessary

 Public bodies should consider public consultations prior to introducing surveillance and inform those impacted once adopted

 The design and operation of surveillance program/practice should minimize privacy intrusion to what is necessary to achieve its goals like designing and installing Surveillance Equipment

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.

**Conclusion:**

Proposed system balances all domains in three dimensions legal, technical and political. In suggested system it has been tried to cover different domains as per present scenario, keeping the fast advancement in technology and emerging domains in the mind. The proposed system has given scope of advancement so that without interfering in other domains new domains can be added. The suggested system has been kept flexible and scalable so that not only present need, but future needs can also be accommodated. Well-structured framework for Privacy is definitely important for an individual but also for society as well as economic growth of country.

**References:**

[1] what is privacy < http://en.wikipedia.org/wiki/Privacy> accessed 11 May 2020

[2] PRIVACY AND HUMAN RIGHTS< http://gilc.org/privacy/survey/intro.html> accessed 10 May, 2020

[3] Privacy-Enhancing Technologies—approaches and development <http://www.sciencedirect.com/> accessed 13 May, 2020

[4] PonnurangamKumaraguru, Privacy in India <http://www.cs.cmu.edu/~ponguru/iaap\_nov\_2005.pdf> accessed 12 May, 2020

[5] The Fading Norm< http://iltb.apargupta.com/2010/03/the-fading-norm/> accessed 09 May, 2020

[6] Privacy and emerging technology : Are Indian laws catching up<http://www.nwmindia.org/Law/Commentary/privacy.htm> accessed 10 May, 2020

[7] Information Technology Act 2000

[8] The Indian Post Office Act, 1898

[9] Code of Criminal Procedure, 1973

[10] The Indian Wireless Telegraphy Act, 1933

[11] Information Security policy and Security Issues <www.alttc.bsnl.co.in/altzine/Vol\_31122005/ns/l2.pps> accessed 12 May, 2020

[12] Central Motor Vehicles Act 1898

[13] MaheshwariVidhan, ‘Article 21 of the Constitution of India: The Expanding Horizons’

<http://www.legalserviceindia.com/articles/art222.htm> accessed 09 May, 2020

[14] Central Motor Vehicles Rule2012

[15] Philip E. Agre, Marc Rotenberg, ‘Technology and privacy: the new landscape’

<http://books.google.co.in/books?id=H2KB2DK4w78C&printsec=frontcover&dq=technology+and+privacy&source=bl&ots=1UZmu8TrQp&sig=YJJNgSU61\_nTcL\_CnCl7Je2LcrQ&hl=en&ei=7L2YS\_T2KYSysgOygbnCAQ&sa=X&oi=book\_result&ct=result&resnum=2&ved=0CAkQ6AEwAQ#v=onepage&q=&f=false> accessed 13 May, 2020

[16] Surveillance< http://en.wikipedia.org/wiki/Surveillance> accessed 09 May, 2020

[17] Bruce Schneier The Eternal Value of Privacy<http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886> accessed 08 May, 2020

[18] Internet privacy< http://en.wikipedia.org/wiki/Internet\_privacy> accessed 08 May, 2020

[19] Electronic Communications Privacy Act <http://legal.web.aol.com/resources/legislation/ecpa.html> accessed 10 May, 2020

[20] ITA Act 2008< http://cactusblog.wordpress.com/2010/01/21/amended-it-act-2008/> accessed 11 May, 2020

[21] Kharak Singh v. The State of U.P. (1962AIR 1295)

[22] People’s Union for Civil Liberties v. Union of India (1996SC 568)

[23]Selvi and others v. State of Karnataka and others (AIR 2010 SC 1974)

[24]Justice K.S. Puttuswamy (Retd.) &Anr. v. Union of India &Ors. (WRIT PETITION (CIVIL) NO 494 OF 2012)

[25]State (N.C.T. of Delhi) v. Navjot Sandhu @ Afsan Guru [(2005)11 SCC 600]

**BRIEF ABOUT AUTHOR**

Bijan Ghosh is a Fifth-year law student at Department of Law, North Bengal University. He is keenly interested in research and scholarship pertaining to Banking law, International Human Rights and Environmental law. Additionally, he is a volunteer of Anti Human Trafficking Club and National Service Scheme.

1. what is privacy < http://en.wikipedia.org/wiki/Privacy> [↑](#footnote-ref-2)
2. MaheshwariVidhan, ‘Article 21 of the Constitution of India: The Expanding Horizons’

   <http://www.legalserviceindia.com/articles/art222.htm> [↑](#footnote-ref-3)
3. Kharak Singh v. The State of U.P. (1962AIR 1295) [↑](#footnote-ref-4)
4. People’s Union for Civil Liberties v. Union of India (1996SC 568) [↑](#footnote-ref-5)
5. Selvi and others v. State of Karnataka and others (AIR 2010 SC 1974) [↑](#footnote-ref-6)
6. Justice K.S. Puttuswamy (Retd.) &Anr. v. Union of India &Ors. (WRIT PETITION (CIVIL) NO 494 OF 2012) [↑](#footnote-ref-7)
7. ITA Act 2008 < http://cactusblog.wordpress.com/2010/01/21/amended-it-act-2008/> [↑](#footnote-ref-8)
8. Ibid [↑](#footnote-ref-9)
9. The Indian Post Office Act, 1898 [↑](#footnote-ref-10)
10. Code of Criminal Procedure, 1973 [↑](#footnote-ref-11)
11. The Indian Wireless Telegraphy Act, 1933 [↑](#footnote-ref-12)
12. Central Motor Vehicles Rule 2012 [↑](#footnote-ref-13)
13. Information Technology Act 2000 [↑](#footnote-ref-14)
14. Supra note 13 [↑](#footnote-ref-15)
15. Surveillance < http://en.wikipedia.org/wiki/Surveillance> [↑](#footnote-ref-16)