

## **E-Privacy and Data Protection in Indian Perspective**

Legal, Technical and Political Challenges, Proposed framework

Mr Vijay chaurasiya(Faculty, Indian Institute of Information Technology, Allahabad)  
Shrikant Ardhapurkar, Tanu Srivastava, Swati Sharma  
MS (Information Security), Indian Institute of Information Technology, Allahabad  
Phone: 91-532-2922000 Fax: 91-532-2430006,contact@iiita.ac.in  
shrikant.999@gmail.com,srivastavtanu@gmail.com,abhswati@gmail.com

**“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 in Indian perspective with respect to challenges in three different dimensions like Legal, Technical and Political domain. We have proposed framework to deal with these challenges. Advancement in technology such as Mobility (Geographic Knowledge Discovery), Data Mining, Cloud computing etc. brings unforeseen challenges and one of the major challenges is threat to “*privacy*”. Today we can access any information related to any one from anywhere at any time but this arise a new threat to private and confidential information. Globalization has given acceptance of technology in the whole world, as per growing requirement different countries has introduced different legal frame work like DPA (Data Protection Act)1998 UK, ECPA(Electronic Communications Privacy Act of 1986) USA etc. from time to time , but in India there is no such comprehensive legal framework that deals with privacy issue. To handle major cyber challenges we refer ITA Act 2008 that was built with the motivation to facilitate e-commerce and hence the privacy was not prior concern in IT act.

This suggestive framework provides comprehensive 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”.

### **(I) Introduction**

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 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” [1]. 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 [16].

Privacy is recognized at international level as Human Rights [2] in different dimension as

- Privacy of person
- Privacy of personal behavior
- Privacy of personal communication
- 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.

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[5][6].

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 some time 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 owner. In the world where data transmission rate is up to 2 terabits per second, the exposure of information occurs in such a fast and vast manner that it is almost impossible to control the flow of information[3].

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 tele caller 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 endeavored to protect at technical side.

There are many organization that are working on globally adapted structure of privacy framework like OECD [39] that has been defined as common platform for countries with common focus, to provide settings to compare policy experiences, seeking

answer to common problem and good practices so that countries can coordinate domestic and international polices, has given prime concern to privacy and proposed guideline to protect privacy that has been adapted by many nations.

Based on OECD [39] guideline UK has adopted DPA (Data Protection Act, 1998) [45] 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.

## **(II) 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 [4].

Certain legislative framework that provides indirect support to privacy concerns in India\_

1. Indian Constitution.
2. IT Act 2000
3. Indian Contract Act 1872
4. Indian Penal Code
5. Indian Copyright Act
6. Consumer Protection Act, 1986
7. Specific Relief Act, 1963
8. Indian Telegraph Act

**IT Act 2000** is introduced to facilitate the e- governance. It provides the wide definition for Information security but Act does not emphasis on Privacy, but there are certain Sections that partially deal with privacy term.

Section 43 of IT act [7]

It mainly provide penalty for the damage of computer system. If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network involves access, downloading, copying of extraction of database including information stored in any removable storage medium is liable to punishable under IT Act. It also covers any type of computer contaminant or computer virus, damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmers residing in such computer, computer system or computer network, disruption, denial of access. It also contain regulation regarding providing an assistance to any person to facilitate access to computer.

Section 65 of IT act [8]

It describes tampering with Computer source Code, whenever anybody knowingly and unknowingly destroys, alters, conceals computer source code when it is maintained by law under observation ,the person shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees,

or with both. Lots of freeware tool are readily available that can decompile source code remotely without the knowledge of source code owner and hence it is very easy to tamper source code in such a manner that it can generate process and transmit information for the unintended purpose and it can leak any ones private information

Section 66 of IT act [9] deals with Hacking. If anyone intentionally cause loss or damage, alters, delete any information by diminishing its value ,commits hacking for example if any sensitive personal email is saved in a computer ,if any person accesses the said document then the value of information is completely lost, this will make the party liable under this provision. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Section 72of IT act [10] deals with penalty for breach of confidentiality and privacy. If any person accesses any e-record, book, information, correspondence without the consent of person whose information is disclosed is punishable act.

*“It is deceptive to compare IT Act with EU directives, Guideline of protection of privacy and Tran’s border flow of personal data 1980 Safe Harbor principal of US”*

**Indian contract Act [11]** is introduced to provide safe agreement between two parties. A contract is a legal agreement between two or more parties .for example buying goods, purchasing items, lending and borrowing a money or ordering machinery from a manufacture are all contract. The term and conditions is decided by the party that is involved in the contract. The parties involved in the contract must adhere with the rules and regulation as specify in the agreement. If the terms and conditions are violated like disclose of information shared between them, causing of damage to other party intentionally under the contract amounts to a breach of the contract.

**Indian Penal Code [12]** made to deal with all crime done in the society. There are certain sections are introduced that partially deals with privacy like Section 406 deals with Punishment for criminal breach of trust, Section 420 applies when any person cheats with other party cause damage, destroy to information ,property is liable under this act.

**Indian Copyright Act [13]** This act provides security to literary, artistic and dramatic, musical work. The copyright act provide right to the original author of above mentioned fields so that no one can misuse their work and maintain the privacy if it is related with some sensitive information and maintain the originality of work.

**Consumer Protection Act [14]** deals with the protection of consumer from exploitation and save them from “deficiency of service such as disclosing proprietary information, personal information etc.without adequate authorization. ”

**Specific Relief Act [15]** provides special relief so that person can claim temporary and permanent injunctions against unauthorized disclosure of confidential information.”

**Indian Telegraph Act [16]** This act refers in case of telecommunication area. Person privacy is fundamental right. But if integrity of nation is breach then Government has power to intercept your communication without your concern.

**Article 21 Act [17]** No person shall be deprived of his life or personal liberty except according to procedure established by law.

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

- There is no comprehensive law and still the privacy issue is dealt with some proxy laws and these proxy laws disperse in different domain and has no convergence on the privacy issue
- There is no classification of Information like public information, private information sensitive information that makes the management of information more complex and hence does not provide specific protection for private information in current legal system.
- There is no legal frame work that talks about ownership of private and sensitive information and data
- There is no certain procedure of creating, processing transmitting and storing the information.
- There is lack of any guideline that defines about Data Quality, Proportionality and Data Transparency.
- There is 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 and clearly depicts the need of codified framework that covers all the privacy issues.

### **(III) Technological challenges**

Globalization and ICT revolution [18] 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.

For that they are transferring their data from paper and file into 0's and 1's thus managing bits has been challenging task since its origin. No one has reckoned that these simple digits can change the life so immensely. Although it has made our life easy, fast and advance but yet it has introduce some unforeseen mayhem and expose our private life. This following has been salient paradigm in ICT revolution:

- The conversion of information in digital form and many complementary technology like EDI (electronic data interchange).
- Introduction in mobility technology like GSM, Geographic knowledge discovery, Bluetooth, RFID (radio frequency identification), etc.
- Internet technology

- Increasing capacity of storage devices with decrease in size even at cheaper cost like micro memory card.

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, Internet Technologies.

Above stated technologies has threatened the privacy up to a great extent as biometric information is exclusively related to an individual and in the case of exposure it can reveal sensitive information about individual and can be misused further. Biometric information threatens the privacy severely.

Latest technologies like RFID has potential risk for privacy due to its small tiny sized tags that can be tagged with anyone and this technology uniquely identifies the individuals and it does customer profiling. This profile can be used for future advertisement target. And with the help of RFID information pooling an individual can be always monitored.

Obviously smart card has made our life easy but it has brought many issues concerning privacy like transaction detail and record can be accessed for unintentional purposes 'whereas credit-card and debit-card generated a trail of 5-10 transactions per month, or perhaps per week, smart card can enable the recording of whereabouts and what you were doing 5-10 times per day' these record may have some private information like frequency and parties of transactions. Even contactless smart card may induce severe invasion to privacy that can be operated without the knowledge of owner.

VoIP depends on Internet Technologies; privacy invader can tap or eavesdrop the private communication and can use this information and cause user's service to collapse.

No doubt wireless has made the access to information more portable but the protocols like WEP on which the security of Wireless network relies itself is obsolete and proved as vulnerable protocol but still being used. The interception on wireless communication is much easier hence sharing private information through wireless can drop off privacy.

New technologies are radically advancing our freedom, but they are also enabling unparalleled invasions of privacy. A very simple and common device cell phone helps you to keep in touch with friends and families, but it also makes it easier for the feds to track your location. Technologies like GPS are sophisticated tracking devices that give extremely detailed, round-the-clock information about the movements of a vehicle or tagged individual has made the tracking of exact position of an individual. In all over world many cases has been sighted in which Location detection technologies has been threat for privacy and national security.

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 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 dataware houses are managed by third parties like BPO etc.

The word *surveillance* comes from the French word for "watching over" [19]. No doubt the purpose of surveillance technology like CCTV is to monitor and prevent unlawful activities but numerous civil rights groups and privacy groups oppose surveillance as a violation of people's right to privacy. Such groups include: Electronic Privacy Information Center, Electronic Frontier Foundation, and ACLU. In Great Britain, for example, which has experimented with the widespread installation of closed circuit video cameras in public places, camera operators have been found to focus disproportionately on people of color, and the mostly male operators frequently focus voyeuristically on women. Surveillance is especially subject to abuse because it can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject. It's possible to put a camera up anywhere and train it on people; modern cameras can easily view faces from over long distance. 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"* [20].

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 [21].

#### **(IV) Political 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. These people are anyone who is responsible for 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.

Here maximum revenue is generated from service sector. Now days IT and ITES services play major role in BPO industries. 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 [5], United State follow ECPA [22]. They do business in India just because investment cost is very low. They due care of their data with compliance of some non-government international organization like ISO [23], ITIL [24] 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.

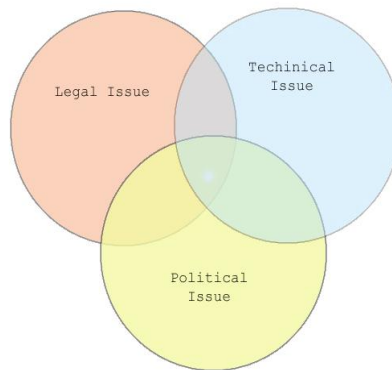
Media play an important role in democracy to make people aware about information related to government policy and what the grievances people have but now a day media encroaches on public life, no one's personal information is kept secure for their own interest. Even media holds no responsibility regarding defense related sensitive information. There must be privacy guideline for media for some special category of information.

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. In social networking sites most community are anti national, which is the hub for Cyber Terrorism. Females and celebrities are always on hits on such community.

Blogs are increasingly popular in today's world. Writing blogs, people can express their thought and their views but in public and government sector every authorize people are writing blogs for reviewing the current policy; make expert comment, critics the work. By there is possibility that private information may be forged and its original intension may be lost.

### (V)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 [12], ITA Act2008 [25], Copyright act [13], Special relief Act [15], Telegraph Act [16] , Contract Act[11], Article 21 [17] and so many other as per of the nature of case. Recently government of India passed special legislation on privacy ITAA 2008 [25] 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) [26] which was initiative by NASCCOM [27]. 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.

In India there is no fast track court to deal with privacy cases. 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.

Although Indian courts have been applying a combination of different laws to ensure protection of data and privacy, absence of effective legislative or judicial measures encourage the blatant misuse of personal information by corporate, banks and telemarketing companies.

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 guaranteed under Articles 19 and 21 of the Constitution of India. (People’s Union for Civil Liberties (PUCL) v. Union of India and Anr. AIR 1997 1 SCC 301.) However, the guidelines issued by RBI in November 2005 are only applied to banks and financial institutions and it did not serve any purpose. The issues remain unresolved and there are public interest litigations pending disposal in the Supreme Court of India seeking protection of privacy rights from UCC. Although the Commission's judgment is of international standards, India should adopt serious measures to prevent UCC. A specific law dealing with UCC, with adequate enforcement mechanism, exemplary damages and fines, provisions for termination of business licenses in case of violation, and penalties for trading of consumers' personal information should be introduced [28].

In current system although the privacy is coupled with Article 21 of Constitution i.e. Right of Liberty under Article 21 of the Constitution of India, an invasion upon one's privacy can be only protected if the offender is the state and not a private entity. If the offender is a private individual then there is no effective remedy except in tort where one can claim damages for invasion in his privacy and no more [29].

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 [30].

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. Efficient working of RTI requires classified information in term of its sensitivity like Public information, Private information, Personal Information, Sensitive Information for this there must be central guideline about information classification [31].

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 [32][33].

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 is third party offshore for processing.[34]

For all SME’s it is very difficult to comply with international standard. To change the image of India from Tech Support to Service Provider there is strong need to develop a privacy frame which copes up all need of information security and privacy of information [35].

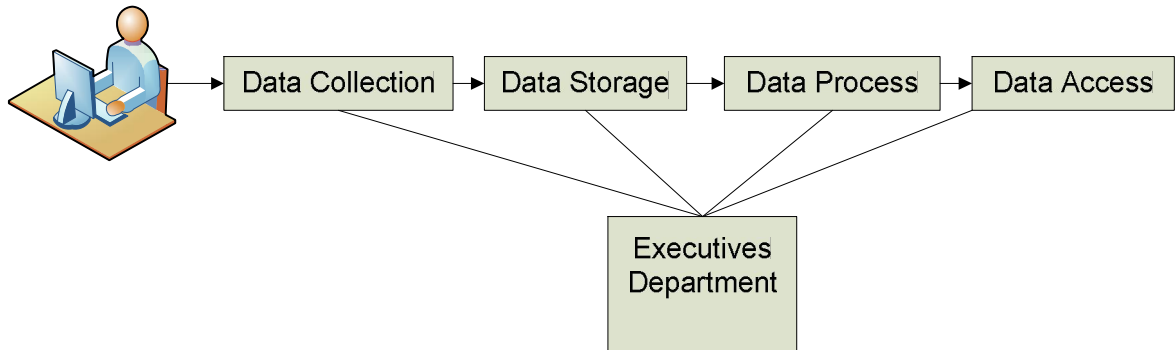
In fact the Information Technology Act, 2000 [36] deals with the issue of data protection and privacy in a bit by bit manner. Presently there is no legal architecture for Data Protection Authority, Data Quality and Proportionality, Data Transparency etc.[37] which properly addresses and covers data protection issues in accordance with the principles of the EU Directive [38], OECD Guidelines[39] or Safe Harbor Principles [40]. Accordingly, even if the new proposed amendments to the Information Technology Act, 2000 [36] 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 treatment .The reason behind that India is a favorable destination because of its infrastructure and technology in which is in par with those in USA, UK and Europe but at comparatively low cost. But lack of privacy guidelines of health related record like HIPAA (Health Insurance Portability and Accountability Act)[41] 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.*"[42]

But still there is no such guideline for health industries to implement health related data privacy protection. Apart from legal framework technology play an important role to protect individual privacy there are variety of privacy enhancing technology (PET) [43]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. The goal of this technology is to increased control over their personal information which is present over the network. It also has data minimization technique i.e. pass on minimum information over the network. It also provides various data tracking system which track your data about its data flow. Main features of this tools is remotely data auditing technique by which data is ensure periodically from safe remote location.

**(VI) Proposed Frame work:**



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 impose 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.
- 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 [44][45]

**(b) Data Security**

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. [44][45]

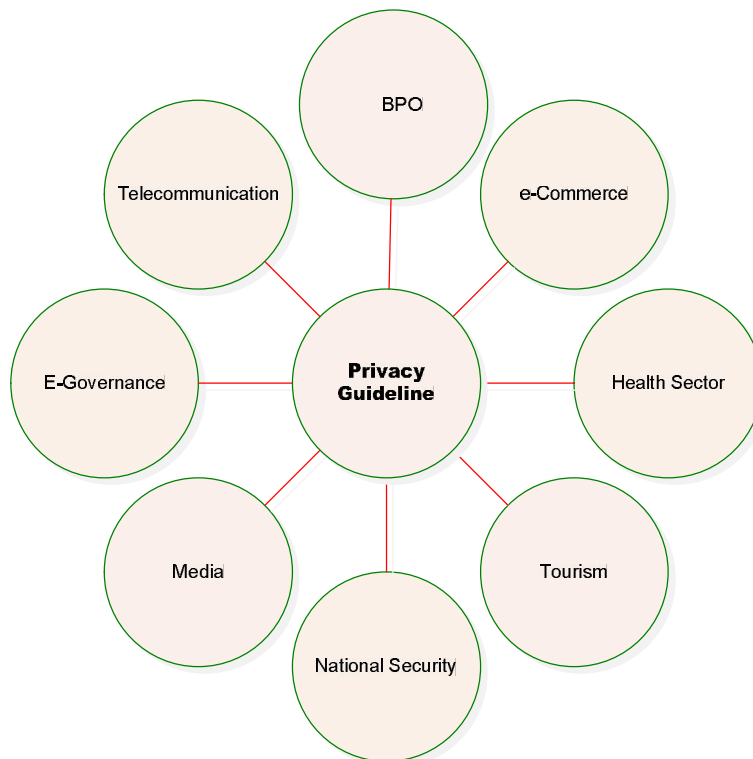
**(c) Data Process**

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. Data shall be processed by data subject accordance with data subject right i.e. data subject have right to the content block the processing and editing in the process flow[44][45]

**(d) 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 they must have to follows all above the norms followed by the Indian government. [44][45]

**Domains Covered in Frame work**



### **(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 [46] [47]like:

- Creating a Union Chief Privacy Officer
- Installing chief privacy officers (CPOs) at all major departments
- Ensuring that Data Mining techniques are addressed by the Privacy Act
- Strengthening and standardizing privacy notices including "privacy impact assessments"
- 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[48]. 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

#### General Principles

The e-court must provide security and privacy of electronic filings. Court shall make any document that is filed electronically publicly available online.” Provided the exceptions by that documents filed but not “otherwise available to the public, such as documents filed under seal, shall not be made available online.” certain categories of documents are not to be included in a public case file and may not be made available to the public either at the court house or via remote electronic access.

These categories are unexecuted summonses or warrants of any kind (e.g., search warrants, arrest warrants); pretrial bail or presentence investigation reports; statements of reasons in the judgment of conviction; juvenile records, documents containing identifying information about jurors or potential jurors financial affidavits in seeking representation [49]

- There must be unified and coherent policy for the privacy protection and access rights applicable for judicial proceeding, case, juror verdict, including the private information.
- Members of the bar must be educated about the policies and the fact that they must protect their clients by carefully examining the documents that they file in court for sensitive, private information and by making the appropriate motions to protect documents from electronic access when necessary.
- Except where otherwise noted, the policies apply to both paper and electronic files.
- The availability of case files at the courthouse will not be affected or limited by these policies.

#### Civil Case Files

That documents in civil case files should be made available electronically to the same extent that they are available at the courthouse with one exception: Social Security cases should be excluded from electronic access; and one change in policy: the requirement that certain personal data identifiers be modified or partially redacted by the litigants. These identifiers are dates of birth, financial account numbers and names of minor children.

#### Criminal Case Files

That public remote electronic access to documents in criminal cases should not be available

#### Bankruptcy Case Files

The documents in bankruptcy case files should be made generally available electronically to the same extent that they are available at the courthouse, with some exceptions for personal identifiers as in civil cases of the bankruptcy code should be amended to establish privacy and security concerns as a basis for the sealing of a document; and that the bankruptcy code .

#### Appellate Case Files

That appellate case files be treated at the appellate level the same way in which they are treated at the lower level.

#### **(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. To cover public grievances there media generally take the public opinion in the form of interviews, press meeting, onsite observation, sometime critics to view by doing this media least bother about privacy of particular individual media is work on commercial basis they are looking for TRP by the race of TRP Media encourage the privacy of individual. 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 must be definition and guide line about privacy protection. There is no guideline to handle this issue privacy frame will provide solution to solve this problem. Framework must give guidance to solve the 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 (NASSCOM)[50], 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."[51]

In India BPO is most popular because processing in India is relatively cheap but there are other countries like China , Philippines are close competitor to India 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. In BPO lots of data travel in different way like data travel through intranet, internet, travel via storage device this leads to breach in privacy there must be policy which deals with privacy issue.

Privacy at work place is also ignored field, thousands of worker 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. If we give legal framework then it helps to boost the BPO sector and it result to generate new source of income.

#### **(e) Telecommunication:**

Service providers (SPs) 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 people and organizations that are allowed to receive, disclosures are prohibited from using the information or documents they have received for purposes other than those for which the information was given. 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.

The main exceptions to the prohibition on disclosure of customer information include[52]:

- where the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or the protection of the public revenue
- where the disclosure is made to the legal proceedings to assist in the consideration of a complaint;
- where the disclosure is required or is otherwise authorized under a warrant or under law
- where the disclosure is for prescribed business needs of other carriers or service providers

#### **(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 dental records
- 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 [41] and PSQIA [ 53] Patient Safety Rule made by US government that establishes a voluntary reporting system to enhance the data available to assess and resolve patient safety and health care quality issues.

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.

### **e-Business**

Indian economy majorly based on e-business outsourcing. Business can be described as the exchange of goods and services between groups, individual for different services. While e-business refers to more strategic focus with an emphasis on the functions that occur with electronic capability, it can also be describes as the utilization of Information and Communication Technology for e-commerce purpose to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers. Exchange of services involve financial transaction, flow of sensitive information etc [54].

Privacy is the major concern for the protection of information regarding e-business domain. 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 and Availability must be ensured, 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. Privacy framework also ensures the proper functioning of e-business model, whether the business is operating between Business-to-Business, Business-to-Customer. If there is a proper privacy framework then proper continuity of business is maintained forever [55][56].

### **(g) 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. People visit in India for the medical purpose that come under the medical Tourism. When tourist visits in India they perform several transaction from the day they entered into our country and enter their sensitive information from booking of tickets, booking of hotels, currency exchange, taking medical facilities, while doing online shopping every where they give their personal information like name, address, contact number, email-id. But there is no guarantee that this provided information is not further misused[57][58].

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[59].

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.

#### **(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.*  
[60]

Using surveillance systems to address concrete, confirmed problems and/or incidents is acceptable only if the practice meets all statutory requirements and is utilized as a last resort outweighing the diminution of personal privacy. The activities like Access, Use, Disclosure, Retention, Security and Disposal of Surveillance Records must be regulated [61]

- 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 absolutely necessary to achieve its goals like designing and installing Surveillance Equipment
- System operators require privacy-sensitivity training
- The safeguarding of the equipment and data and images must occur
- After making the decision to use surveillance, the public body should adopt comprehensive policies and procedures to direct the program/practices
- Surveillance programs/practices should be subject to audit and evaluation

The word security derive from the word *securus* which means carefree .The definition of the security often begin with free from danger, risk ,etc; safety. 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.[62]

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. Government must have separate body that deals with National Security and privacy framework apart from Intelligence authority. 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

The proposed system covers all domains in three dimensions legal, technical and political .In proposed system it has been tried to cover various 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 proposed 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 economical growth of country.

## Acknowledgement

We are grateful to Dr. M.D Tiwari (Director), Dr. Anurika Vaish(Divisional head) in Indian institute of Information Technology Allahabad for their informative guidance.

## References

- [1] <http://en.wikipedia.org/wiki/Privacy>
- [2] PRIVACY AND HUMAN RIGHTS  
<http://gilc.org/privacy/survey/intro.html>
- [3] Privacy-Enhancing Technologies—approaches and development  
<http://www.sciencedirect.com/>
- [4] Ponnurangam Kumaraguru, Privacy in India  
[http://www.cs.cmu.edu/~ponguru/iaap\\_nov\\_2005.pdf](http://www.cs.cmu.edu/~ponguru/iaap_nov_2005.pdf)
- [5] The Fading Norm  
<http://iltb.apargupta.com/2010/03/the-fading-norm/>
- [6] Privacy and emerging technology : Are Indian laws catching up?  
<http://www.nwmindia.org/Law/Commentary/privacy.htm>
- [7] IT Act 2000, Gazette of India Part 2 –Section 1,Pg 22
- [8] IT Act 2000, Gazette of India Part 2 –Section 1,Pg 29
- [9] IT Act 2000, Gazette of India Part 2 –Section 1,Pg 29
- [10] IT Act 2000, Gazette of India Part 2 –Section 1,Pg 31
- [11] Indian Contract Act 1872, ACT No. 9, 1872
- [12] The Indian Penal Code 1860, ACT No. 45, 1860
- [13] Indian Copyright Act 1957  
<http://www.majmudarindia.com/pdf/Data%20Protection%20in%20India.pdf> [Majmudar & Co Majmudar & Co., International Lawyers, India]
- [14] Information Security policy and Security Issues  
[www.alttc.bsnl.co.in/altzine/Vol\\_31122005/ns/12.pps](http://www.alttc.bsnl.co.in/altzine/Vol_31122005/ns/12.pps)
- [15] Information Security policy and Security Issues  
[www.alttc.bsnl.co.in/altzine/Vol\\_31122005/ns/12.pps](http://www.alttc.bsnl.co.in/altzine/Vol_31122005/ns/12.pps)
- [16] Article 21 of the Constitution of India: The Expanding Horizons (Maheshwari Vidhan)  
<http://www.legalserviceindia.com/articles/art222.htm>
- [17] ITA Act 2000[25]  
<http://www.majmudarindia.com/pdf/Amendments%20to%20the%20Information%20Technology%20Act%20and%20data%20privacy%20issues.pdf>
- [18] Philip E. Agre, Marc RotenbergTechnology 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](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)

- [19] Surveillance  
<http://en.wikipedia.org/wiki/Surveillance>
- [20] Bruce Schneier The Eternal Value of Privacy  
<http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886>
- [21] Internet privacy  
[http://en.wikipedia.org/wiki/Internet\\_privacy](http://en.wikipedia.org/wiki/Internet_privacy)
- [22] Electronic Communications Privacy Act  
<http://legal.web.aol.com/resources/legislation/ecpa.html>
- [23] ISO  
<http://www.iso.org/iso/home.html>
- [24] ITIL  
<http://www.itil-officialsite.com/home/home.asp>
- [25] ITA Act 2008  
<http://cactusblog.wordpress.com/2010/01/21/amended-it-act-2008/>
- [26] DSCI  
[http://www.dsci.in/images/stories/dsci\\_brochure\\_24th\\_july\\_2009.pdf](http://www.dsci.in/images/stories/dsci_brochure_24th_july_2009.pdf)
- [27] NASSCOM  
[http://www.nasscom.org/.../Annexure\\_1\\_Indian\\_Security\\_Environment\\_Dec\\_2007.doc](http://www.nasscom.org/.../Annexure_1_Indian_Security_Environment_Dec_2007.doc)  
<http://www.dsci.in/>
- [28] <http://www.majmudarindia.com>,  
 Pdf: Telecom companies and protection of Personal data in India
- [29] White Paper on Privacy Protection in India :Vakul Sharma  
<http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf>
- [30] Controversy Of Love And Libel: Sagarika Ghose  
<http://www.outlookindia.com/article.aspx?200468>
- [31] [www.rti.org.in](http://www.rti.org.in)  
 News on Right to Information: compiled by Ms. M. Shanthi, Manager (Knowledge Resources)
- [32] Article: Data Protection Law In India-Needs And Position(Adv. Swati Sinha)  
<http://www.legalserviceindia.com/article/l368-Data-Protection-Law-In-India.html>
- [33] <http://bpo.tcp.in/>  
 Fake it and you break it by: Sunder Ramachandran
- [34] [www.intertek-sc.com/our\\_services/ISO\\_27001/](http://www.intertek-sc.com/our_services/ISO_27001/)  
 Article : Information Security Management Systems: ISO 27001
- [35] Article: The Impact of ISO Implementation on Output Parameters in SME's in India  
 Singh,L.P. Bhardwaj,A. Sachdeva, A. Nat. Inst. of Technol., Jalandha <http://ieeexplore.ieee.org/>
- [36] IT Act 2000, Gazette of India Part 2 –Section 1
- [37] Article:” Does India have a Data Protection law?”( Mohammed Nyamathulla Khan)  
<http://www.legalserviceindia.com/article/l406-Does-India-have-a-Data-Protection-law.html>
- [38] EU Directives  
[http://ec.europa.eu/justice\\_home/fsj/privacy/lawreport/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm)
- [39] OECD Guidelines  
<http://www.oecd.org/dataoecd/56/36/1922428.pdf>
- [40] SAFE HARBOR PRIVACY PRINCIPLES  
[http://www.coe.int/t/e/legal\\_affairs/legal\\_co-operation/data\\_protection/documents/national%20laws/IUSA\\_SAFE%20HARBOR%20PRIVACY%20PRINCIPLES.pdf](http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national%20laws/IUSA_SAFE%20HARBOR%20PRIVACY%20PRINCIPLES.pdf)
- [41] HIPAA  
<http://privacyruleandresearch.nih.gov/>
- [42] White Paper on Privacy Protection in India (Vakul Sharma)  
<http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf>
- [43] Data Protection Technical Guidance Note: (PET) Privacy enhancing technologies (ICO)  
[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/privacy\\_enhancing\\_technologies.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf)
- [44] Information Sheet (Public Sector) 1-Information Privacy Principles under the Privacy Act 1988  
<http://www.privacy.gov.au/materials/types/infosheets/view/6541>
- [45] Data Protection Act 1998: 1998 CHAPTER29  
[http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)

- [46] Policies and Guidelines for Effective e-Governance (Gopala Krishna Behara) (Madhusudhana Rao) <http://www.egovonline.net/articles-list/47-features/7426-policies-and-guidelines-for-effective-e-governance-.html>
- [47] E-Government Act Section 208 Implementation Guidance [http://www.whitehouse.gov/omb/memoranda\\_m03-22/](http://www.whitehouse.gov/omb/memoranda_m03-22/)
- [48] E-Courts In India <http://www.groundreport.com/Opinion/E-Courts-In-India/2912646>
- [49] Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files <http://www.privacy.uscourts.gov/crimimpl.htm>
- [50] Working with India (publisher: Springer Berlin Heidelberg, ISBN no: 978-3-540-89077-5 (Print) 978-3-540-89078-2 (Online), page no: 63-94, date: Tuesday, November 18, 2008) <http://www.springerlink.com/content/k124647232575302/?p=a9e53d399b8a49be9a41f86d96dcb4ea&pi=3>
- [51] Under Pressure, India Mulls Steps to Protect Privacy (Vir Singh) <http://spectrum.ieee.org/telecom/security/under-pressure-india-mulls-steps-to-protect-privacy>
- [52] Review of the Telecommunications (Interception) Act 1979 <http://www.efa.org.au/Publish/efasubm-agd-tiactreview2005.html>
- [53] Patient Safety and Quality Improvement Act of 2005 (PSQIA) <http://www.hhs.gov/ocr/privacy/psa/understanding/index.html>
- [54] e-Business Anup Ghosh, Security & Privacy for E-Business ISBN No. 0-471-38421-6 ,Publisher: John Wiley & Sons , <http://www.cigital.com/books/secpriv/>
- [55] e-Business Paul Shaw, E-Business Privacy and Trust: Planning and Management Strategies, ISBN: 978-0-471-21811-1, Published July 2002
- [56] About the PCI Data Security Standard (PCI DSS) [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)
- [57] Tourism In India [http://en.wikipedia.org/wiki/Tourism\\_in\\_India](http://en.wikipedia.org/wiki/Tourism_in_India)
- [58] Medical tourism <http://www.medicaltourismmag.com/issue-detail.php?item=51&issue=3>
- [59] Tourism In Dublin <http://www.visitdublin.com/Information/Default.aspx?id=341>
- [60] Bob Whitehead, Invasion of privacy laws and video surveillance -- what's legal, what's not? <http://www.video-surveillance-guide.com/3048-invasion-of-privacy-laws.htm>
- [61] Roger Clarke Visual Surveillance and Privacy <http://www.rogerclarke.com/DV/VisSurv0508.html>
- [62] Tracy Mitrano, Civil Privacy and Legislative Security Policy <http://net.educause.edu/ir/library/pdf/ERM0362.pdf>