Challenging the Scenario of Privacy in Indian Online Market

*Mr. Susil Kumar Sarangi * & Dr.DibakarPanigrahy **

Abstracts

According to a report provided by Forrester Research, e-commerce revenues in India will increase by more than five times by 2016, jumping from USD 1.6 billion in 2012 to USD 8.8 billion in 2016.The growth of the e-commerce industry over the last few years is definitely undisputable, at the same time it is important to understand that success stories of e-commerce as a model have been observed in certain specific industries. According to recent news reports, the travel industry accounts for nearly three-fourths of the commerce that takes place online (approximately 71 % and e-tailing taking the second spot with a small share of 16%.The fact that only a small market share is attributable to the e-tailing industry does not defy the growing influence that online shopping has on people. In the initial years e-tailing seemed more popular for purchase of computer products and it still does contribute to a majority of e-tailing, but lifestyle shopping seems to be the new found trend for internet users. These businesses have capitalized on the convenience factor that online trading offers to customers and this has been the success mantra not just for Flipkart but host of other websites. It is in this context that online privacy is main block to the growth of online business. Given the dynamic nature of the onlinesphere, privacy concerns and issues are rapidly changing. Transactions on the internet, particularly consumer- related transactions, often occur between parties who have no pre-existing relationship.

Internet privacy encompasses a wide range of issues and topics. It can be understood as privacy rights that an individual has online with respect to their data, and violations of the same that take place online. This may raise concerns of the person's identity and authenticity with respect to issues of the person's capacity, authority and legitimacy to enter the contract. Though the Internet eliminates the need for physical contact, it does not do away with the fact that any form of contract or transaction would have to be authenticated and in certain instances recorded. Different authentication technologies have evolved over a period of time for authenticating documents and also to ensure the identity of the parties entering into online transactions.

Key Words: Online privacy, Regulatory Issues, authenticity,e-tailing

---

Introduction:

Today the number of internet users in the world is close to 3 billion. Out of this, India has a total of 259.14 Million internet and broadband subscribers. This penetration of internet coupled with the increasing confidence of the internet users to purchase online, has led to an enormous growth in the e-commerce space, with an increasing number of customers registering on e-commerce

websites and purchasing products through the use of mobile phones. It is not surprising; therefore, that India is in a prime position for the growth and development of the e-commerce sector. In particular, e-commerce presents one of the greatest opportunities in the retail sector since it provides a dramatic change from brick and mortar establishments to virtual shops which could operate for a fraction of the cost. According to a report provided by Forrester Research, social networks play an important role in driving consumers online and getting them to engage with brands. This would gain specific significance in light of facts such as India being ranked as Facebook's second largest audience after the US. However, it should be kept in mind that there still exists a form of 'digital divide' in India where the benefits of internet have not fully percolated to non-urban areas. In this scenario, mobile connections would play a very important role. India has close to 914.92 Million wireless subscribers. Mobile phones have been and will be a key tool in helping users connects in a market where overall internet penetration may be low.

Objective of the Study: The main objective of this descriptive research is to analyze that reflect the present situation in Indian Context. Our research provides information about the current situation and focus on history, current and future online data privacy. This study tries to analyze the following important topics concerned with the growth of online marketing.

1. Security concerns.
2. Privacy of Data
3. Jurisdiction on privacy
4. Policies on Privacy of other countries
5. Expert group recommendations on privacy

Types of Privacy

The term privacy can have different meaning in different context. Peoples have different opinion and views on what they can term as the breach of their privacy rights.

Personal Privacy:

The main and the most related term in the context of privacy can be related to the exposure of one's body to another, it can also be defined as physical privacy. This is also an expect of personal modesty. A personal can go to extreme depth in order to protect his modesty. Like one wears clothes to prevent his body to be seen to others, creates walls or fences etc. People also expect that their privacy rights will be respected by others too. "Intrusions into one's physical space or solitude" This would include such concerns as:

1. Preventing intimate acts or hiding one's body from others for the purpose of modesty; apart from being dressed this can be achieved by walls, fences, privacy screens, cathedral glass, partitions between urinals, by being far away from others, on a bed by a bed sheet or a blanket, when changing clothes by a towel, etc.; to what extent these measures also prevent acts being heard varies

a. Video, of aptly named graphic, or intimate, acts, behaviors or body parts
b. Preventing unwelcome searching of one's personal possessions
c. Preventing unauthorized access to one's home or vehicle.
d. Medical privacy, the right to make fundamental medical decisions without governmental coercion or third party review, most widely applied to questions of contraception.

Informational Privacy:

As the term says informational privacy is related to information or data about a person. This data can be of any type and in any form for example name, date of birth, address, phone number, bank details etc. The concern of privacy arises in collecting, storing and sharing of personal data.

Organizational Privacy:

Various organizations, agencies or corporations may desire to keep their activities hidden from other organizations or individuals. Like the defense or military department etc. They can implement various methods to achieve their desired privacy.

Privacy and the Internet

Internet has almost changed the way one used to fear from privacy invasion. Peoples are harassed and blackmailed on social networking sites. Their photos are downloaded, morphed and misused. Though Internet has revolutionized the world and it has become a global village now, on the other hand we cannot deny the negative aspects of it. We need to understand the fact that everything that we do on internet can be noticed or revealed because it leaves digital traces. The use of smart phones is another emerging danger to online privacy. Every device that is connected to Internet has a unique IP address attached to it, whether it is a computer, mobile, play station or anything else which means it can be traced. If one doing online transaction or simply anything related to e-commerce it is much possible that one's credentials can be compromised. Now days even if onesearches anything on Google and after some time if one want to search the same thing it will appear in the search drop list even if onetypes the first word of the letter.

Five most dangerous threats to online privacy

One of the most controversial topics in our always-online, always-connected world is privacy. Even casual computer users have become aware of how much "they" know about our online activities, whether referring to the National Security Agency spying on U.S. citizens, or the constant barrage of ads related to something we once purchased.Concerns over online privacy have brought different responses in different parts of the world. In the U.S., for example, many Web browsers let users enable a Do Not Track option that tells advertisers not to set the cookies through which those advertisers track their Web use. Compliance is voluntary, though, and many

parties have declined to support it. On the other hand, European websites, since 2012, have been required by law to obtain visitors informed consent before setting a cookie, which usually means there is a notice on the page saying something like by continuing to use this site, one's consent to the placing of a cookie on one's computer.

1. Cookie proliferation

Marketers say that they keep user data private by viewing it only in aggregate, but the sheer volume of data a cookie can collect about any one person can enable the cookie's owner to infer a surprising amount about the individuals being tracked. As a 2010 report by an US report found, the more that personal information can be correlated, the less it is possible to completely anonymize.

2. Seizing cloud data

One love how easy it is to grab data from the cloud—and so do law enforcement agencies. And there's only going to be more of that data to love in coming years. It is predicts that 36 percent of U.S. consumer content will be stored in the cloud by 2016. But whether one use a Web-based email service, keep files in Google Drive, or upload photos to Shutter fly, everything one write, upload, or post gets stored in a server that belongs to the online service. Data stored in the cloud isn't legally protected in the same way that it would be if it were located on a storage device one own.

3. Location data betrayal

Location data will make it increasingly difficult to wander around the world without someone knowing exactly where one is at any given time. One cell phone is the primary tattletale, but the location data one post to social networking sites are revealing sources too. Pinpointing one whereabouts will get easier still as other location-beaming devices come online, from smarter cars to smarter watches to Google Glass. One cell phone is a prime source of personal location data. And as with cloud-based data, the legal requirements for obtaining location data from one mobile service provider are not terribly stringent. It's pretty easy for the government to get access to the location data, and very hard for users to prevent that data from being gathered. There may not be much one can do about one employer. Reining in the government's zeal for location data may be tough as well. It's such a useful tool for law enforcement to get access to this info, there's a lot of pushback,

4. Data never forgets a face

Posting and tagging photos online may feel like innocent fun, but behind the scenes it helps build a facial recognition database that makes escaping notice increasingly difficult for anyone. Most

consumers are already in the largest facial recognition database in the world, and that's Facebook. Companies such as Google and Apple have facial-recognition technology built into some of their applications, too—most notably online photo sites. The future of facial recognition offers scant comfort. Continued advances in surveillance technology, including drones and super-high-resolution cameras, will make identifying individuals in public places easier than ever, especially if the entity doing the surveillance has a nice, fat, facial-recognition database to consult.

5. Scanning in the name of cyber security

One may not be a malicious hacker, but that doesn't mean one's online activity won't be scanned for telltale signs of cybercrime. Even though the data is supposed to be scanned only in aggregate (so as not to pinpoint individuals), the methodology used in choosing and storing the data raises additional privacy issues.

Legal Regime to Combat Cyber Privacy in India

Let us understand what the legal provisions on Cyber Privacy in India are.

1. Information Technology Amendment Act, 2008:Information Technology Act is an act of Indian Parliament notified on 17, October, 2000. It was further amended and came into force on October 27, 2009. It regulates the cyberspace in India and provides rules and regulations regarding different aspects of cyber law.

Section 43(A): Compensation for failure to protect data:Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Section 66(E): Punishment for violation of privacy**:**Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. Explanation - For the purposes of this section--

(a) "Transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "Capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "Private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

d) "Publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "Under circumstances violating privacy" means circumstances in which a person can have a

reasonable expectation that--

(i) He or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 72: Breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72(A): Punishment for Disclosure of information in breach of lawful contract:Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

These are the sections which provide a citizen some rights to fight for his privacy in IT Act. Also it provides some procedure and rules for monitoring and collecting traffic data or information.

2. Indian Penal Code, 1860: There are some sections in IPC which deals with privacy. They are not directly related with cyber privacy but can be helpful for an individual to claim his or her rights. Like Section 499 – Defamation, Section 500 – Punishment for Defamation, Section 292 – Sale, etc., of obscene books etc., Section 447 – Punishment for Criminal Trespass, Section 509 - Word, gesture or act intended to insult the modesty of a woman.

3.Code for Criminal Procedure, 1973: Few of the sections in CrPC can also be implied with the other sections in other Acts such as Section 320 - Compounding of offences. Right to Information Act, 2005 Section 8 - Exemption from disclosure of information.

4. The Privacy Protection Bill (2013): As the bill says that it is a bill "to establish an effective regime to protect the privacy of all persons and their personal data from Governments, public authorities, private entities and others, to set out conditions upon which surveillance of persons and interception and monitoring of communications may be conducted, to constitute a Privacy Commission, and for matters connected therewith and incidental thereto"

Data Privacy in the U.S

The U.S. relies more on a self-regulatory model, while Europe favors explicit laws. An example of the self-regulatory model is the Advertising Self-Regulatory Council (ASRC) administered by the Council of Better Business Bureaus. The ASRC suggests placing an icon near an ad on a Web page that would link to an explanation of what information is being collected and allow consumers to opt out; however, there is no force of law behind the suggestion. while the formal U.S. regulatory system is much less restrictive than the European approach, the fines handed down by the U.S. Federal Trade Commission—which is charged with overseeing what privacy regulations there are—are much harsher than similar fines assessed in Europe.The Obama administration, in a January 2012 white paper titled Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy outlined seven privacy principles and proposed a Consumer Privacy Bill of Rights (CPBR). It stated that consumers have a right:

1. To expect that data collection and use will be consistent with the context in which consumers provide the data,
2. To secure and responsible handling of personal data,
3. To reasonable limits on the personal data that companies collect and retain,
4. To have their data handled in ways that adhere to the CPBR,
5. To individual control over what personal data companies collect from them and how they use it,
6. To easily understandable and accessible information about privacy and security practices, and
7. To access and correct personal data in usable formats.

The CPBR itself takes a two-pronged approach to the problem: it establishes obligations for data collectors and holders, which should be in effect whether the consumer does anything or even knows about them, and "empowerments" for the consumer. The obligations address the first four principles in the list, while the empowerments address the last three.

Data Privacy in Europe

The 2000 Charter of Fundamental Rights of the European Union has explicit provisions regarding data protection. Article 8 says,"Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone

has the right of access to data which has been collected concerning him or her, and the right to have it rectified."In 1995 directive of the European Parliament and the Council of the European Union, read, "Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms." These documents establish the EU-wide framework and foundation for online privacy rights.The roots of the concernlie in the countries' memory of what happened under Nazi rule. They understand that state surveillance is not only a matter of what the government does, but that a private company that holds the data can give it to the government. Consequently, the EU is concerned with anyone that collects and tracks data, while in the U.S. the larger concern is government surveillance rather than corporate surveillance.

The EU's principles cover the entire Union, but it is up to individual countries to carry them out in practice. Implementation and enforcement varies from country to country. In Spain, Google is suffering a lot, but it's not happening so much in Ireland. In December 2013, the Spanish Agency for Data Protection fined Google more than $1 million for mismanaging user data. In May 2014, the European Court of Justice upheld a decision by the same agency that Google had to remove a link to obsolete but damaging information about a user from its results; in response, Google set up a website to process requests for information removal, and by the end of that month claimed to have received thousands of requests.

Online Privacy in Japan

The legal framework currently governing data privacy in Japan is the 2003 Act Concerning Protection of Personal Information. The Act requires businesses handling personal information to specify the reason and purpose for which they are collecting it. It forbids businesses from changing the information past the point where it still has a substantial relationship to the stated use and prohibits the data collector from using personal information more than is necessary for achieving the stated use without the user's consent. The Act stipulates exceptions for public health reasons; among others. The Japanese government was expected to revise the 2003 law, due to the fact that new technologies have weakened its protections. Changes probably will be influenced by both the European Commission's Data Protection Directive and the U.S. Consumer Privacy Bill of Rights (as outlined in the Obama administration white paper), as well as by the Organization for Economic Co-operation and Development (OECD) 2013 privacy framework.

In preparation for such revisions, the Japanese government established a Personal Information Review Working Group. Some Japanese privacy experts advocate that the U.S. Consumer Privacy Bill of Rights and FTC (Federal Trade Commission) staff reports can be applied in the revision, but for now these attempts have failed. Meanwhile, Japanese Internet companies are arguing for

voluntary regulation rather than legal restrictions, asserting such an approach is necessary for them to be able to utilize big data and other innovative technologies and to support international data transfer.As one step in this process, the Japanese government announced a policy outline for the amendment of these laws in June 2014. The main issue up for revision is permitting the transfer of de-identified data to third parties under the new third-party authority. The third-party authority would be an independent body charged with data protection. No one is sure whether this amendment would fill the gap between current policy and the regulatory approaches to online privacy in the EU and U.S.The Japanese government gathered public comments, including a supportive white paper from the American Chamber of Commerce in Japan which, unsurprisingly, urged that any reforms take the least restrictive approach, respect due process, [and] limit compliance costs.

Internet Privacy in India

In relation to an e-commerce business, processing payments forms a vital part of the transaction and in this regard various payment systems to carry on an e-commerce business have also developed. In fact the IT Act gives legal recognition to the authentication of any information by affixing an electronic signature as long as it is in compliance with the manner as prescribed under the IT Act. Further, the IT Act also provides the regulatory framework with respect to electronic signatures including issuance of electronic signature certificates.The way in which the internet allows data to be produced, collected, combined, shared, stored, and analyzed is constantly changing and re-defining personal data and what type of protections personal data deserves and can be given. The seemingly harmless data such IP address, key words used in searches, websites visited, can now be combined and analysed to identify individuals and learn personal information about an individual. From information shared on social media sites, to cookies collecting user browser history, to individuals transacting online, to mobile phones registering location data – information about an individual is generated through each use of the internet. In some cases the individual is aware that they are generating information and that it is being collected, but in many cases, the individual is unaware of the information trail that they are leaving online, do not know who is accessing the information, and do not have control over how their information is being handled, and for what purposes it is being used. In fact the law enforcement agencies routinely troll social media sites for information that might be useful in an investigation. In India, in 2013 the Mumbai police established a "social media lab" for the purposes of monitoring and tracking user behavior and activities. In the U.S, individuals have contested the use of their tweets without permission, while courts in the US have ruled that tweets, private and public, can be obtained by law enforcement with only a subpoena, as technically the information has been shared with another entity, and is therefore no longer private. Indian Courts have yet to deal directly with the

question of social media content being public or private information.

The Complication of Jurisdiction

The borderless nature of information flows over the Internet complicates online privacy, as individual's data is subjected to different levels of protection depending on which jurisdiction it is residing in. Thus, for example an Indian using Gmail, will be subject to the laws of the United States. On one hand this could be seen as a positive, if one country has stronger privacy protections than another, but could also be damaging to privacy in the reverse situation – where one company has lower privacy standards and safeguards. In addition to the dilemma of different levels of protection being provided over data as it flows through different jurisdictions, access by law enforcement to data stored in a different jurisdiction, or data from one country accessible to law enforcement because it is being processed in their jurisdiction, are two other complications that arise. These complications cannot be emphasized more than with the case of the NSA Leaks. Because Indian data was residing in US servers, the US government could access and use the data with no obligation to the individual. In response to the NSA leaks, the government of India has stated that all facts need to be known before any action is taken, while citizens initially sought to hold the companies who disclosed the data to US security agencies such as Google, Facebook etc. accountable.

Current Policy for Internet Privacy in India

Currently, India's most comprehensive legal provisions that speak to privacy on the internet can be found in the Information Technology Act (ITA) 2000. The ITA contains a number of provisions that can, in some cases, safeguard online privacy, or in other cases, dilute online privacy. Provisions that clearly protect user privacy include: penalizing child pornography, penalizing, hacking and fraudulent defining data protection standards for body corporate. Provisions that serve to dilute user privacy speak to access by law enforcement to user's personal information stored by body corporate collection and monitoring of internet traffic dataand real time monitoring, interception, and decryption of online communications. Additionally, legislative gaps in the ITA serve to weaken the privacy of online users. For example, the ITA does not address questions and circumstances like the evidentiary status of social media content in India, merging and sharing of data across databases, whether individuals can transmit images of their own "private areas" across the internet, if users have the right to be notified of the presence of cookies and do-not track options, the use of electronic personal identifiers across data bases, and if individuals have the right to request service providers to take down and delete their personal content.

Online Data Protection

As mentioned above, India's most comprehensive data protection standards are found in the ITA and are known as the Information Technology "Reasonable security practices and procedures and sensitive personal data or information" Rules 2011. The Rules seek to provide rights to the individual with regards to their information and obligate body corporate to take steps towards protecting the privacy of consumer's information. Among other things, the Rules define "sensitive personal information' and require that any corporate body must publish an online privacy policy, provide individuals with the right to access and correct their information, obtain consent before disclosing sensitive personal information ' except in the case of law enforcement, provide individuals the ability to withdraw consent, establish a grievance officer, require companies to ensure equivalent levels of protection when transferring information, and put in place reasonable security practices. Though the Rules are the strongest form of data protection in India, they have not been recognized by the European Union as meeting the EU standards of data secure and many gaps still exist. For example, the Rules apply only to:

1. Body corporate and not to the government
2. Electronically generated and transmitted information
3. A limited scope of sensitive personal information.
4. A body corporate when a contractual agreement is not already in place.

These gaps leave a number of bodies unregulated and types of information unprotected, and limit the scope of the Rules. It is also unclear to what extent companies are adhering to these Rules, and if they are applying the Rules only to the use of their website or if they are also applying the Rules to their core business practices.

Future frameworks for privacy in India: Justice A.P.Shah Report

In October 2012 the Report of the Group of Experts on Privacy was published by a committee of experts chaired by Justice A.P. Shah. The report creates a set of recommendations for a privacy framework and legislation in India. Most importantly, the Report recognizes privacy as a fundamental right and defines nine National Privacy Principles that would apply to all data controllers both in the private sector and the public sector. In addition to defining principles, the Report recommends the establishment of a privacy commissioner for overseeing the implementation of the right to privacy in India and specifies that aggrieved individuals can seek redress either through issuing a complaint the privacy commissioner or going before a court. The nine national privacy principles include:

Principle 1: on Notice: A data controller shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is

collected from them. Such notices should include:

1. during Collection

a. What personal information is being collected;

b. Purposes for which personal information is being collected;

c. Uses of collected personal information;

d. Whether or not personal information may be disclosed to third persons;

e. Security safeguards established by the data controller in relation to the personal information;

f. Processes available to data subjects to access and correct their own personal information;

g. Contact details of the privacy officers and SRO ombudsmen for filing complaints.

2. Other Notices

a. Data breaches must be notified to affected individuals and the commissioner when applicable. Individuals must be notified of any legal access to their personal information after the purposes of the access have been met.

b. Service providers would have to explain how the information would be used and if it may be disclosed to third persons such as advertisers, processing. Individuals must be notified of changes in the data controller's privacy policy.

c. Any other information deemed necessary by the appropriate authority in the interest of the privacy of data subjects.

Implications: A telecom service provider must make available to individuals a privacy policy before any personal information is collected by the company. For example, the service provider must identify the types of personal information that will be collected from the individual from the initial start of the service and during the course of the consumer using the service. Such as from name and address to location data with a notice if information will be disclosed to third parties such as advertisers, processers, or other telecom companies. If a data breach that was the responsibility of the company takes place, the company must notify all affected customers. If individuals have their personal data accessed or intercepted by Indian law enforcement or for other legal purposes, they have the right to be notified of the access after the case or other purpose for the data has been met.

Principle 2: on choice and consent

A data controller shall give individuals choices with regard to providing their personal information, and take individual consent only after providing notice of its information practices.

Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies. When provision of information is mandated by law, it should be in compliance with all other National Privacy Principles. Information collected on a mandatory basis should be anonymized within a reasonable timeframe if published in public databases. As long as the additional transactions are performed within the purpose limitation, fresh consent will not be required. The data subject shallalso have an option to withdraw his/her consent given earlier to the data controller. In such cases the data controller shall have the option not to provide goods or services for which said information was sought if such information is necessary for providing the goods or services. In exceptional cases, where it is not possible to provide the service with choice and consent, then choice and consent should not be required.

Implications: If an individual is signing up to a service, a company can only begin collecting, processing, using and disclosing their data after consent has been taken. The provision of information is mandated by law, as is the case for the census, this information must be anonymized after a certain amount of time if it is published in public databases. Suppose there is a case where consent is not possible, such as in a medical emergency, consent before processing information, does not need to be taken.

Principle 3: means of Collection of Information

A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.

Implication: If a bank is collecting information to open an account for a potential customer, they must collect only that information which is absolutely necessary for the purpose of opening the account, after they have taken the consent of the individual.

Principle 4: On Purpose alterations

Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles.

Implication: If a bank is collecting information from a customer for opening a bank account, the

bank can only use that information for the purpose of opening the account and any other reasons consented to. After a bank has used the information to open an account, it must be destroyed. If the information is retained by the bank, it must be done so with consent, for a specific purpose, with the ability of the individual to access and correct the stored information, and in a secure fashion.

Principle 5: On Access and Correction

Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data. Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, unless that person has explicitly consented to disclosure.

Implications: An individual, who has opened a bank account, has the right to access the information that was initially provided and subsequently generated. If there is a mistake, the individual has the right to correct the mistake. If the individual requests information related to him that is stored on a family member from the bank, the bank cannot disclose this information without explicit consent from the family member as it would impact the privacy of another.

Principle 6: On Disclosure of Information to third parties

A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.

Implications: Now a website, like a social media site, collects information about how a consumer uses its website, this information cannot be sold or shared with other websites or partners, unless notice of such sharing has been given to the individual and consent has been taken from the individual. If websites provide information to law enforcement, this must be done in accordance with laws in force, and cannot be done through informal means. The social media site would be prohibited from publishing, sharing, or making public the personal information in any way without obtaining informed consent.

Principle 7: On Security of data

A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorized access, destruction, use,

processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.

Implications: If a company is a telecommunication company, it must have security measures in place to protect customers' communications data from loss, unauthorized access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure, or other foreseeable risk. This could include encrypting communications data, having in place strong access controls, and establishing clear chain of custody for the handling and processing communications data.

Principle 8: On Openness to sensitivity

A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

Implications: If a hospital is collecting and processing personal information of 1,000 patients, their policies and practices must reflect and be applicable to the amount, sensitivity, and nature of information that they are collecting. The policies about the same must be made available to all individuals – this includes individuals of different intelligence, skill, and developmental levels.

Principle 9: On Accountability for compliance

The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.

Implications: To ensure that a hospital is in compliance with the national privacy principles, it must undertake activities like running trainings and providing educational information to employees on how to handle patient related information, conducting audits, and establishing an officer or body for overseeing the implementation of privacy.

Observations

For many years there has been running public discourse about the surveillance that the Indian government has been undertaking. This discourse is growing and is now being linked to privacy and the need for India to enact privacy legislation. As discussed above, the current surveillance regime is lacking on many fronts, while at the same time the government continues to seek greater interception powers and more access to larger sets of information in more granularity.

Projects like the Central Monitoring System, NATGRID, and Lawful Interception Solutions have caused individuals to question the government on the proportionality of State surveillance and ask for comprehensive privacy legislation that also regulates surveillance.

Since 2010, there has been a strong public discourse around the need for privacy legislation in India. In November 2010, a "Privacy Approach" paper was released to the public which envisioned the creation of data protection legislation. In 2011, the Department of Personnel and Training released a draft privacy bill that defined a privacy regime that encompassed data protection, surveillance, and mass marketing, and recognized privacy as a fundamental right. In 2012 the Report of the Group of Experts on Privacy, was published.Presently, the Department of Personnel and Training is drafting the text of the Governments Privacy Bill. In 2013, the Centre for Internet and Society drafted the Citizen's Privacy Protection Bill – a citizen's version of privacy legislation for India. From April 2013 – October 2013, the Centre for Internet and Society, in collaboration with the Federation of Indian Chambers of Commerce and Industry and the Data Security Council of India, held a series of seven Privacy Roundtables across India. The objective of the Roundtables was to gain public feedback to a privacy framework in India.

Conclusion

With the world's data borders becoming ever more permeable even as companies and governments collect more and more data, it is increasingly important that different regions are on the same page about these issues. With the U.S. trying to satisfy EU requirements for data protection, and proposed reforms in Japan using the EU's principles and the proposed U.S. "Make no mistake, everything we touch that is digital in the future will be a data source." Clearly, privacy is an emerging and increasingly important field in India's internet society. As companies collect greater amounts of information from and about online users, and as the government continues to seek greater access and surveillance capabilities, it is critical that India prioritizes privacy and puts in place strong safeguards to protect the privacy of both Indians and foreigners whose data resides temporarily or permanently in India. The first step towards this is the enactment of a comprehensive privacy legislation recognizing privacy as a fundamental right. The Report of the Group of Experts on Privacy and the government considering a draft privacy bill are all steps in the right direction.The need for strong and enforceable surveillance provisions is not unique to India, and in 2013 the International Principles on the Application of Human Rights to the Surveillance of Communications were drafted. The principles lay out standards that ensure that surveillance is in compliance with international human rights law and serve as safeguards that countries can incorporate into their regimes to ensure the same. The principles include: legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification,

transparency, and public oversight, integrity of communications and systems, safeguards for international cooperation, safeguards against illegitimate access. Along with defining safeguards, the principles highlight the challenge of rapidly changing technology and how it is constantly changing how information can be surveilled by governments and what information surveilled by governments, and how information can be combined and analysed to draw conclusions about individuals.

Assistant Professor,
P.G. Department of Business Administration,
Kalam Institute of Technology, Berhampur,
Odisha; PIN: 761003

****Professor,***
P.G. Department of Business Administration,
Kalam Institute of Technology,Berhampur
University, Berhampur,
Odisha. PIN: 760007

References:

1. 'Trends in India's e-Commerce Market': Report provided by Forrester Research for ASSOCHAM's 2nd National Conference on e-Commerce 2012.
2. Indian-ecommerce-market-to-reach-20-billion-next-year-rep.html (last visited on January 22, 2015)
3. Mellissa Reofrio-"5 biggest online threat of 2013"The Telegraph
4. Logan Kugler "Online Privacy: Regional Differences" Communications of the ACM, Vol. 58 No. 2, Pages 18-20.
5. Alan D. Smith, "Cybercriminal impacts on online business and consumer confidence", Online Information Review Volume 28 · Number 3 · 2004 · pages. 224–234, 2004
6. Alan F. Westin, "Privacy and Freedom", Bibliography: pages. 445-458, 1967
7. Alessandro Acquisti, "Privacy and Security of Personal Information Economic Incentives and Technological Solutions", J. Camp and R. Lewis (eds), The Economics of Information Security, Kluwer, 2004
8. Alessandro Acquisti; Allan Friedman; Rahul Telang, "Is there a Cost to Privacy Breaches? An Event Study" Twenty Seventh International Conference on Information Systems, Milwaukee 2006 and Workshop on the Economics of Information Security, Cambridge, UK, 2006
9. Andreas M. Antonopoulos, "The black market for identity theft Security: Risk and Reward",
10. Cyber Privacy Issues In India by Rehan Umar Khan, Student at National Law Institute University, Bhopal