CONSUMER PRIVACY

Contents

Introduction

Traditionally speaking, and according to the Consumer Protection Act, 1986, in India, a consumer is a broad label for any person who buys goods or services with the intent of using them for non-commercial purposes.[1] In the typical sense, when people think of themselves as being consumers, they think about transactions with a vendor through a physical exchange of money in a store or through an online exchange for a product or service. Certain services that consumers use put an extraordinary amount of sensitive personal information into the hands of vendors. For example, the information that hospitals, banks and telecommunications collect during transactions is highly sensitive. For companies, consumer privacy is typically approached in terms of economic value — trying to find the balance between the right to privacy and positive economic growth. Once collected, a consumer's data can be used for legitimate purposes (research, etc.) and illegitimate purposes (data mining, etc). Specific ways in which consumer privacy can be compromised include: behavioural advertising, mis-management of sensitive personal information, and data breaches and data leaks. Increasingly, data that is collected from consumers are stored in databanks created by both private and public entities. The mass consolidation of consumer information increases privacy and security concerns. Thus, for the individual, consumer privacy is concerned with the manner in which information that has been disclosed to a vendor is collected, used, stored, shared and destroyed. In other words, strong protection of consumer privacy requires strong data protection principles. This chapter will examine the present legal state of consumer privacy in India and seek to understand the gap between policy and implementation of policy. In doing so, it will look at what are the existing avenues for protection of consumer privacy in India, how is the definition of consumer privacy evolving through case law and public opinion, and what are the current challenges to consumer privacy in India.

Six potential avenues for the protection of consumer privacy in India

1. *The Consumer Protection Act:* Individuals can seek compensation for a deficiency in service or for 'unfair trade practices' under the Act.
2. *Privacy Policies*: Individual organizations commit to protect the information of their clients through "Privacy Policies". Organizations are not required by law to follow an organizational wide privacy policy. Thus, any adherence to a privacy policy is voluntary.
3. *Contract:* Organizations enter into contract with individual clients. Within these contracts are guidelines as to how an individual's privacy will be protected. The creation of a contract is found under the Indian Contract Act, 1872, and is enforced through civil litigation.
4. *Codes of conduct:* Professions and industries like the medical profession, the legal profession, the banking industry, and the telecom industry have codes of privacy that are created by the respective governing bodies and statutorily enforced. These guidelines are enforced through penalties for breach including loss of license and monetary penalties.
5. The Information Technology Act, 2000: The Sensitive Personal Information Rules notified in 2011[2] impose an obligation on organizations to protect personal sensitive information that is collected and provide remedy against losses caused by the leakage or improper use of data. For a more detailed discussion please see the Internet and Communications chapter.

6. *Tortious Liability:* In some cases individuals can use the tort of breach of confidentiality to claim compensation for misused information.

Legislations

Indian Contract Act, 1872

This Act was enacted for the purpose of regulating the formation of legal contracts in India. The Act came into force on September 1, 1872. It extends to the whole of India [except the State of Jammu and Kashmir] (Subs. by Act 3 of 1951, sec. 3 and Sch., for "except Part B States")[3].The Act creates monetary penalties for breach of contract by individuals, companies, and government departments etc.[4], and clarifies what is a contract, what is a proposal, and what constitutes acceptance and consent. Contracts are critical to privacy as an individual is constantly entering into contracts everyday and consenting to different terms of service and use of information as they complete transactions online and offline. The Act itself does not directly say anything about privacy but there are provisions within the Act which could be important to an individual for protecting privacy when entering into a contract. These include:

Contract: Any agreement which is enforceable by law is a contract. An agreement is every promise and set of promises forming the consideration for each other, a promise is made when a proposal is accepted. A proper offer and acceptance, free consent, valid consideration (cash, etc), competent capacity, lawful object, and the intention to create legal relationship.[5]

Consent: Consent is defined as two or more persons who agree upon the same thing in the same sense.[6]

Free Consent: Consent is free when it is not caused by 1) coercion, undue influence, fraud, misrepresentation, and mistake. Coercion[7] is defined as the committing or threatening to commit any act forbidden by the Indian Penal Code or the unlawful detaining, or threatening to detain, any property, to the prejudice of any person whatever, with the intention of causing any person to enter into an agreement. Undue influence is defined as a contract that is induced by undue influence where the relations subsisting between the parties are such that one of the parties is in a position to dominate the will of the other, and uses that position to obtain an unfair advantage over the other.[8] Fraud is defined and includes someone with the intent to deceive another party by 1) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true, 2) the active concealment of a fact by one having knowledge or belief of the fact, 3) a promise made without any intention of performing it, 4) any other act fitted to deceive and 5) any such act or omission as the law specially declares to be fraudulent.[9] Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud. Misrepresentation includes 1) positive assertion in a manner not warranted by the information of the person making it, of that which is not true, though he believes it to be true, 2) any breach, of duty which, without an intent to deceive, gains an advantage to the person committing it or any one claiming under him, by misleading another to his prejudice or to the prejudice of any one claiming

under him, and 3) causing, a party to an agreement to make a mistake as to the substance of the thing which is the subject of the agreement.[10]

Standards for acceptance: Acceptance must be absolute, unqualified and must be expressed in some usual and reasonable manner, unless the proposal prescribes the manner in which it is to be accepted. [11]

When a contract is considered voidable: A contract which arises from during coercion, fraud, misrepresentation, or when consent is given under undue influence, or when there is a mistake as to matter of fact by both the parties, such contract is considered voidable.[12]

Changes or substitution of a contract: If the parties to a contract agree to substitute or alter a contract – it is not necessary to carry out the original contract.[13]

Liability of person to whom money is paid or service delivered by coercion or mistake: If mistake is made and a service incorrectly delivered, the person who has mistakenly received the information must return it.[14]

Compensation: When there is a breach in contract, the party who suffers direct loss by such breach is entitled to receive compensation from the party who breached the contract.[15] If a contract contained a penalty for breach, the party complaining of the breach is entitled to the sum of the penalty, even if damage was not caused.[16]

Third party liability: When two persons contract with a third person, the third person is only liable to the most relevant contract.[17\

Misrepresentation or concealment of terms of service: If a company misrepresents or conceals by keeping silent components of their terms of services, any guarantee made is invalid.[18]

Liability for a change in terms of contract without consent obtained: An individual cannot be held liable for any change made to a contract without his/her consent. For example, a bank changes their policy on overdraft fees without taking consent from the individual for the new policy, the individual cannot be held responsible for overdraft fees incurred under the new policy.[19]

Return of goods after completion of specified purpose: Goods must be returned on expiration of time or accomplishment of the purpose for which the information was required.[20]

Acts done without consent or knowledge: When acts are done by one person on behalf of another but without his knowledge or consent, he may ratify the act.[21]

In light of the fact that the Act does not contain specific provisions pertaining to the right of privacy, in our research we sought to understand what possible protections an individual could have through a contract. In doing so, we interviewed Anjana Thomas, partner at the Indo Juris Law offices, who answered these questions for us:

1. **Can an individual give up their right to privacy by signing a contract?**
   There is nothing in the Contract Act that expressly provides that an agreement through which a person gives up his/her right to privacy is void. Individuals can contract out personal rights, but cannot contract out rights that impact public policy, for example, one cannot contract out their right to life.
2. **If a company makes changes to a contract, do they need to obtain new consent from the client?**
   Unilateral changes to an agreement without obtaining fresh consent are not enforceable under the Contract Act, unless a new contract and new consent is taken. Under Indian law there cannot be a valid contract without consensus to the terms of the contract between the parties. However, acceptance of the changes proposed does not necessarily need to be in writing, because the Indian Contract Act recognizes implied acceptance by conduct. Therefore, if an individual is aware of the changes and continues to perform under the modified contract, they could be held to have impliedly accepted the changes.
3. **If work is subcontracted out in the delivery of a service then who is held liable for a deficiency — the original company or the third party?**
   If work is sub-contracted out, the remedy for breach of the contract will be with the original company who was a party to the agreement, and not the third party sub-contractor. Unless it is the intention of the parties to a contract that the contract will be performed by the company itself, the promise may be sub-contracted by the original company without being in breach of contract.
4. **Under the Contract Act, if I enter into an agreement with a company and in the agreement they agree to protect my information — but my information is stolen, can I seek remedy under the Contract Act?**
   If a company agrees to protect an individual's information but fails to do so, the company has broken the contract, and therefore the individual is entitled to receive compensation for loss or damage. The exact nature of the obligation undertaken by the organization with respect to the information needs to be determined. For example, if the organization only agrees to take reasonable security measures to secure the information and did so, but the information was stolen none the less, then the bank would not be in breach of its obligation under the contract. Therefore, the individual would have no remedy against the bank.
5. **Does the Contract Act cover contracts between foreign nationals and Indian Companies vice versa?**
   The Contract Act is applicable throughout India and does not distinguish between the nationalities of the contracting parties. Thus, the Contract Act could apply to contracts between foreign nationals and Indian companies. To determine the place of an online contract, it is necessary to look into the Code of Civil Procedure, 1908 and determine where the cause of action was.[22] Typically the courts will determine which law will apply. As a note, online services often have a 'jurisdiction' clause and an 'applicability' of law clause. Furthermore, it is often the case that when a company is contracting across countries, it is possible for the company to decide which law is applicable and in which jurisdiction the case will be heard — so a case could be heard in India, using US law.

6. **If a contract is inaccessible or not understandable to the common man — can it be held void under the Contract Act?**
   Generally no, though there some specific exceptions. Typically a person of sound mind is normally bound by his signature on a document whether he reads it, or understands it or not. The law does not generally save a person from his mistake in signing an agreement without understanding it. For a contract to be voidable, a person would need to show coercion, fraud, undue influence, or misrepresentation. If a person alleges coercion, fraud, undue influence, misrepresentation etc., the person must prove it. There are certain exceptions in the Indian context though. For example, if a *pardanishin* woman, who is illiterate and unaware of the contents of the document that she signed, seeks to avoid the contract, the burden of proving that she knew what she was signing and that there was no fraud etc., shifts to the other party.
7. **What is the maximum amount of compensation that a person can claim under the Contract Act?**
   There is no quantification of the amount of compensation under the Contract Act. A person however, has the right to be compensated for any loss or damage he suffers as a result of the other party breaking the contract. The compensation cannot be for remote / indirect loss but only for (i) loss that naturally arose in the usual course, or (ii) which parties knew would be likely to result when they made the contract.
8. **If a company is acquired, what happens to my contract?**
   There is no provision addressing this question in the Contract Act. However, when a company is acquired by another — there are two ways in which this can happen: a.) the acquired company ceases to exist and its assets and liabilities come to vest in the acquiring company. In this case, the acquiring company would be a successor-in-interest, and steps into the shoes of the acquired company. Your contract would then be responsible for the contracts entered into by the acquired company. b.) The acquired company does not cease to exist, but some part of its business is transferred to the acquiring company. In this case, what happens to the contract entered into by the acquired company will depend on the terms of the acquisition — the original company could continue to be responsible for the contract. Or, if the contract relates to the part of the business that is acquired, the new company may step into the shoes of the original company.

The Consumer Protection Act, 1986 (2002)

This Act was passed with the objective to protect the interests of the consumer. In doing so the Act has the potential to protect the privacy of a consumer. For instance, the Act protects against 'unfair trade practices', provides multiple avenues for consumer complaints to be made, and establishes multiple redressal and consumer rights enforcement councils. The purpose of these councils is to protect different consumer rights which include the right to safety, choice, representation, redressal, and education. The councils that are found at the state and national level, are quasi-judicial bodies, and have the ability to issue civil fines. The stated objectives of the Act are to:

- Protect against the marketing of goods which are hazardous to life and property.
- Promote the right to be informed about the quality, quantity, potency, purity, standard, and price of goods to protect the consumer against unfair trade practices.
- The right to be assured that consumers interests will receive due consideration at appropriate forums.
- The right to seek redressal against unfair trade practices or exploitation through a district, state, or national level tribunal.

Complaints under the Consumer Protection Act are allowed in the following circumstances:

- A trader / service provider adopts an unfair trade practice or a restrictive trade practice;
- Goods purchased that suffer from defects;
- Services that suffer from deficiency;
- Excess charges; and
- Goods / services are hazardous / unsafe (injury to life / safety).

Under the Act, “defect” is defined as: fault, imperfection or shortcoming in quality, quantity, potency, purity or standard of goods. “Deficiency” is defined as: fault, imperfection or shortcoming in quality nature or manner of performance of service. “Unfair trade practice”: relate to false or misleading representations with respect to the goods/services.

Like with the Contract Act, the Consumer Act does not speak directly to privacy. Thus, in our research we asked questions pertaining to the redress that an individual can seek under the Act. Namely we asked:

- Can a consumer seek redress under the Consumer Act if a company misuses their information?
- Can a consumer seek redress under the Consumer Act if a company does not have a clear or accessible policy?

We received varied responses to these questions. On one hand, according to Anjana Thomas, services often do not directly pertain to the use of information. Thus, the only way that a complaint with respect to information could potentially lie, would be to make a case that the service was provided contrary to the manner in which the service provider had agreed to provide the services. For example, if one of the conditions of the service was confidentiality of the information and this clause is breached. However, how this would be accepted needs to

be seen. Thus, in case the information is a fundamental part of the services (e.g. say someone who is providing service relating to processing of services) it may be easier to sustain a consumer complaint. In others, a plea could be taken that it does not relate to quality, etc., of the goods/services themselves and therefore, is not a consumer complaint maintainable under the Consumer Protection Act. On the other hand, individuals who participated in the conference 'Consumer Privacy' in New Delhi on July 7, 2012[23] maintained that if an organization has committed to protect information and, even if it does not explicitly say so in the terms of service, if the company fails to protect information an individual can take the complaint to the consumer court. In the conference it was also proposed by participants that instead of passing a privacy legislation, it could be sufficient to amend the Consumer Protection Act in such a way as to mandate data protection and provide privacy protection to the consumer protection.

Tortious Liability

As explained by Justice P. Singh in his book *The Law of Torts*, in India the courts have recognized the tort of confidentiality and that there are situations outside of a contract where an obligation for confidentiality is necessary and where there does not necessarily need to exist between parties as the law places a duty of confidence on information that an individual receives that he knows, or ought to know is to be kept confidential. This is typically information about an individual's private life. For example, relationships which give rise to obligations of confidence include: professional relationships, commercial, matrimonial, and political. Singh also explains that the Tort of confidentiality can be overridden by a higher duty, for example, an auditor discovered that an employee is committing fraud, he has a duty to report this immediately. Furthermore, the tort of confidentiality can be extended into the right of privacy. Examples of cases where breach of confidentiality have been used include:

Zee Telefilms vs. Sundial Communications[24]

In this case Sundial Communications asked the court for an ad-interim injunction restraining Zee Telefilms on the grounds of misuse of confidential information and copyright infringement of Sundial Communications' original work "*Krishna Kanhaiya*". In this case, Sundial Communications, a media company had developed a presentation for Zee Telefilms with the understanding that it was confidential. Later, Zee Telefilms used a close version of the material in the presentation and claimed it as their own original work. In the case, the court held that Sundial Communications did have a case of breach of confidentiality and that the work of the defendants was similar in material and substantial aspects with that of the plaintiffs. In coming to this conclusion the courts reasoned that for an expectation of confidentiality over information to exist, three circumstances would have to be met 1. the release of information would cause injury to the owner or give advantage to his rivals, 2. the owner must believe that the information is secret and is not already in the public domain, 3. belief in 1 & 2 must be reasonable.[25] Furthermore, the court went on to define breach of confidence highlighting that: 1. there is a broad understanding that information received in confidence should not be misused, 2. if any other individual besides the owner wishes to use the information, consent must be obtained.[26]

Mr. Diljeet Titus, Advocate vs. Mr. Alfred Adebare[27]

In this case an employee was fired in March 2004 and took with him a copy of confidential information from the company. While making their decision the court took five aspects into consideration: (1) the law applicable and the content and nature of the relationship, (2) if a relationship as a partner was present, (3) whether payment received from other firms would

affect the merits of the controversy, (4) whether breach of confidentiality has an independent cause of action and (5) whether the company can establish that they are the authors of the document.[28] In its decision the court held that the case of the defendant was clearly falling within the parameters of 'breach of trust or confidence'.[29]

Professional Codes

Certain professions and industries have codes of privacy that they must statutorily abide by. This is true for professions such as medical, legal, banking, telecom, etc. Privacy norms are set for each of these industries by their respective governing bodies. Penalties for breach may include loss of license and monetary penalties.

Advocates

Rules of professional conduct have been framed under the Advocates Act, 1961 which establishes a code of conduct to be followed by lawyers in order to protect the confidence, information, and data of a client. It is important to note that the obligation of confidentiality continues even after the client relationship is ended. Complaints of 'professional misconduct' against advocates are referred to a disciplinary committee constituted under Section 36B of the Advocates Act, 1961 which is empowered to impose a range of sanctions from censure to suspension to striking the advocate off the rolls of the bar council.[30]

Medical Practitioners

In 2002, the Medical Council of India notified the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 which contain ethical injunctions backed by disciplinary action in cases of breaches. Several of these relate to privacy and have been discussed previously in this report in the context of medical privacy.

Banking and Telecom Industry

The banking and telecom industries have regulatory authorities which have periodically issued guidelines seeking to protect the privacy of customers. Thus, for instance, Reserve Bank of India (RBI)'s customer service statement obliges bankers to maintain secrecy, and not to divulge any information to third parties. Likewise, the Telecom Regulatory Authority of India (TRAI) has issued regulations on unsolicited commercial communications and has initiated steps to monitor confidentiality measures taken by telecom operators. For more information with regards to the protections established by the TRAI and RBI, please see the Financial Privacy and Internet and Telecommunications chapter.

Self Regulation

Data Security Council of India

In addition to the legal modes of privacy protection, there are many groups and bodies in India that work towards protecting consumer privacy by encouraging the adoption of strong data protection principles. The most influential and prominent body working on the promotion of data protection principles for the private sector is the Data Security Council of India (DSCI).The council was set up as an independent self regulatory organization for the purpose of promoting data protection, developing security and privacy codes, and encouraging the IT/BPO industry to implement good security practices. Specific to privacy, DSCI promotes nine principles for organizations to adhere to: notice, choice and consent, collection limitations, use limitation, access and correction, security, disclosure to third parties, openness and accountability. These principles are yet to have legal backing in India and are promoted through self regulatory mechanisms by DSCI.[31] Though more organizations are adopting the principles, mostly organizations within the IT sector take efforts to apply the principles. Eventually DSCI hopes to establish and implement a self regulatory model of privacy compliance, similar to ones followed in Canada or Japan. Under such a model, industry bodies such as the RBI or TRAI would be responsible to holding companies in that sector compliant with data protection standards while DSCI would act as a central organization and liaison with the government — establishing different policies and codes to be enforced.

Consumer Groups

Complementing the broad overarching privacy work that DSCI does within the industry, there are numerous grassroots consumer protection groups and consumer activists that work at the grassroots level in protecting consumer privacy. These groups work to help individuals exercise their rights and seek redress for violation. For example, the Citizen Consumer and Civic Action Group (CAG), based in Chennai is a non-profit, non-political and professional organization that works towards protecting citizens' rights in consumer and environmental issues and promoting good governance processes including transparency, accountability and participatory decision-making. Among their initiatives, the group focuses on promoting consumers rights to information, choice, representation, and redressal.[32]

Many organizations also take it upon themselves to incorporate privacy into their organizational structures. An example of an organization that has done this is GSMA mobile. GSMA mobile has created a standard mobile privacy framework that the company strives to adhere by. The principles do not have legal backing, but are designed specifically to protect mobile user's privacy. The principles include: openness, transparency, and notice, purpose and use, user choice and control, data minimization and retention, respect for users' rights, security, education, protection of children and adolescents, and accountability and enforcement.[33]

Case Laws

The case law that emerges pertaining to a certain right is one of the most accurate ways to measure how a right is actually taking shape and being defined in society. In India there is very little case law related directly to consumer privacy, but there are two important cases that do help one extract a definition of what consumer privacy means in India.

Rajinder Nagar Post Office vs. Sh. Ashok Kriplani[34]
In this case a post master was accused of not delivering a registered letter, opening it, and then returning it in a torn condition. It was determined that the tearing of the letter without delivery to addressee was a grave "deficiency in service" on the part of the appellant. It was ruled that the right of privacy of the respondent was infringed upon by the postman. Under the Consumer Protection Act, 1986, a compensation of Rs. 1000 was awarded as to the mental agony, harassment, and loss arising from the charge of deficiency in service. The importance of this case lies in the willingness of the courts to treat breach of privacy as a "deficiency of service".

Airtel, ICICI, & American Express – Unsolicited calls:[35]
In January 2007, the Delhi State Consumer Disputes Redressal Commission imposed a fine of Rs. 75 lakh on a group of defendants including Airtel, ICICI and the American Express Bank for making unsolicited calls, messages and telemarketing. The decision was later reversed on appeal to the Delhi High Court.

These two court cases begin to shape a definition of consumer privacy that includes: 1. a deficiency of service is an invasion of privacy, and 2. un-consented invasions into private space is an invasion of a consumer's privacy. Thus, privacy is both concerned about a person's physical space and about how personal property is treated in professional transactions.

Implementation

Privacy Policies and Terms of Service

Several Indian companies have publicly stated privacy policies on their website:

Airtel

Airtel, an Indian service provider in its privacy policy defines personal information, informs users how their information will be used, and describes which third parties will have access to personal information, provides the ability to opt-out of commercial SMSes, and provides a contact address for individuals who have privacy concerns.[36]

Rediff

The Rediff website states what personal information will be collected from individuals, what information will be stored, what information is collected by cookies, who will collect the personal information, how the information will be used to promote tailored advertising, etc. It states the rights that advertisers have to personal information, provides a disclaimer of responsibility for any other websites linked to the page, states that the information released in a chat room is considered public information, defines third party usage, defines security measures taken, lays out what choices the consumer has regarding collection and distribution of their information, contains opt-out clauses, and explains that consumers have the ability to correct inaccurate information.[37]

Times of India

The Times of India website is owned by Bennett Coleman & Co, and in the privacy policy clearly states that the site will collect information supplied by users and information automatically tracked while navigating the site. The policy also states that by using the website, one is consenting to the collection, storage, and use of the personal information one provides. This will include email address, password, age, PIN code, credit card details, medical records and history, sexual orientation, password, occupation, interests, etc. All information provided on the site is considered in the public domain. Additionally, the website also uses cookies, allows third parties to link to the website, and states that it shares personal information without obtaining consent with law enforcement and internally.[38]

Credit Information Bureau (India) Limited (CIBIL)

The website of CIBIL does not have a privacy policy, but it does include a terms of service. In the terms of service, it clearly states that CIBIL is not responsible for the accuracy or completeness of the information provided, CIBIL does not need to seek prior permission before updating information, and that CIBIL is not liable for any loss caused by error or mistake, CIBIL is not responsible for returning documents or information back to the client.[39]

Hathway

Hathway internet services contain a privacy policy and terms of service on their website. The privacy policy states that information will only be disclosed to conform to legal requirements, protect and defend Hathway's interests, and enforce the terms and conditions. Collection of information is on a need to know basis.

Privacy policies are still not widespread in India though as many companies do not have privacy policies on their websites. Examples of Indian organizations without privacy policies posted on the website include Canara Bank, Andhra Bank, Indian Railways, Air India, Bharat Sanchar Nigam Limited, and State Bank of India.

Behavioural Advertising

Behavioural advertising is a growing trend, used to generate ads alongside search results. Companies match the advertisements to the content of the page that the consumer is viewing. Information collected from these sites is non-personally identifying information and typically includes IP host address, date, time, and time zone of the ad request, pages viewed, browser type, the referring url, and the computer's operating system. Behavioural advertising raises privacy concerns because companies use collected information to create behavioural profiles, which can then be used for secondary purposes and bodies such as credit and insurance companies.

Technology used by behavioural advertising networks includes Ad Tags, API, Web Beacons & Pixels, and Cookies. Ad Tags are pieces of code that allow for the delivery of online advertisements in dedicated ad spaces on websites and in online applications. According to one company, PubMatic, they use Ad Tags transmit anonymous information about the website, section of the site, and size of the ad that is being optimized back to the hosting company. According to PubMatic's privacy policy, API's are application programming interfaces that allow a software program to access and make use of another software program. APIs are used by companies for real time bidding services and to download unique publisher data. Cookies on the other hand are used by companies to collect and send information about a user's website visit. For example, a cookie will collect number of visits, average time spent, pages viewed, navigation history through the website, and other statistics. This information can be used to improve a user's online experience by saving passwords, or allowing companies to track and improve website loading times. Lastly, Web Beacons & Pixels can be used for site traffic reporting, unique visitor counts, advertising auditing and reporting, personalization, and other uses. Most pixels collect only anonymous data, and are placed by online data collecting companies. If consumers wish to stop the collection of personal information, some companies offer ‘opt in’ or ‘opt out’ choices. Choosing the ‘opt out’ choice means that an ‘opt out’ cookie will be placed on your computer, and tell the website not to collect information for the purpose of tailoring advertisements.[40]

A few examples of advertising companies in India include: Komlu, PubMatic, PayPod, IndiaAds, and Sulekha AdNetwork. From a review of these companies’ websites, only a few were transparent about their practices. PubMatic, a company that is based in the US and markets to India, is one of the more transparent companies. PubMatic is an ad network aggregator that works with a number of publishers and data providers. PubMatic is in compliance with US Safe Harbour standards. PubMatic collects IP host address, date, time, and time zone of the ad request, pages viewed, browser type, the referring url, and the computer operating system from users. This information is stored for 90 days, anonymised, and aggregated.[41]

In India there are no rules or guidelines explicitly regulating online behavioural advertising, thus it is not entirely clear what practices different companies and internet service providers

(ISPs) undertake, what information is collected, how the information is used, how long the information is stored for, and what access law enforcement has to this information.

Data Centres

A recent news item from Information Week reported on the rapid creation of data centres in India. Data centres store and process outsourced data from different companies, allowing companies to focus on their core functions and objectives. The article found that many of the data centres followed (ISO) standards and certifications as well as TIA/ANSI-942 and Tier certifications.[42] For example, Reliance Communications operates nine data centres across India. Each data centre provides hosting, network, application, and consulting services to the customer, and offers space, power, cooling, and other needed facilities for companies to come and install and operate equipment. Reliance also offers companies the option of storing their data on the cloud, and offers central computing plus data storage and IT infrastructure hosting.[43]

International Best Practices

Australia

The Privacy Act 1988

In the Australian privacy regime the Office of the Privacy Commissioner is combined with the Office of the Australian Information Commissioner and is an independent statutory office.[44] Australia has both a Federal Privacy Act and Commissioner, and state and territory level Privacy Acts and Commissioners.[45] State and territory level legislation focuses on privacy and the public sector and in some cases interception, surveillance, health, and work place privacy. Enforcement of the privacy regime focuses on voluntary compliance with judicial enforcement reverted to when necessary. The role of the Federal Commissioner includes:

- *Audits*: audits, examination of records, and privacy impact assessments.[46]
- *Clarification of Privacy Principles:* Provision of non-binding guidance which offers definitive interpretations of the rights and obligations of parties flowing from the privacy principles. The commissioner also has the ability to approve/revoke privacy codes and review the operation of approve privacy codes, and examine proposed enactments that might interfere with the privacy rights of an individual.[47]
- *Own Motion Investigation*: Investigate an act or practice of an agency that may breach an Information Privacy Principle and reach a settlement through conciliation.[48] If the commissioner investigates on its own motion, it may issue a report of its findings to a minister if it finds further action is necessary.[49]
- *Investigation into Complaints:* Individuals may issue complaints to the Privacy Commissioner. The commissioner may address the concern or transfer it to the appropriate body.[50] For the purposes of investigation the commissioner has the power to obtain documents, examine witnesses, and direct individuals and attend compulsory conferences.[51]The determination of the commissioner is non-binding and needs to be taken to the court and backed by a court decision.

- *Public interest determinations:* The commissioner has the ability to determine if an act that is in breach of a privacy principle or code is acceptable as the act is in the interest of the public.[52]
- *Education*: The commissioner has the responsibility of promoting an understanding of the Information Privacy Principles, research and monitor developments in data processing and computer technology, and prepare and publish guidelines to assist organizations in applying privacy codes, deal with complaints, etc.[53]
- *Advice:* To provide advice to a minister, agency, or adjudicator on the operation of this Act.[54]
- *Maintenance of Record:* Prepare and maintain a record of the matters set out in records maintained by record keepers.[55]
- *Communicate with Ministers:* The commissioner may inform a minister of an action that needs to be taken by an agency for compliance to be met.[56]
- *Examine Proposals for Data Linking:* To examine a proposal for data linking or matching that may interfere with the privacy of an individual.[57]
- *Issuance of guidelines:* The commissioner is responsible for issuing guidelines for the Data-Matching Program (Assistance and Tax) Act 1990 and the National Health Act 1953.[58]
- *Recommendations:* The commissioner may make reports and recommendations regarding the desirability of legislative or administrative action needed.[59]
- *Responsibilities to certain sectors*: The commissioner has additional responsibilities in relation to: personal property securities, credit reporting, healthcare identifiers, tax file numbers, human rights issues, social interests, and various international obligations.[60]

United Kingdom

The UK Data Protection Act 1998

The United Kingdom (UK) data protection regime is enforced by the officer of the information commissioner, the information tribunal, and data controllers. The commissioner's decisions are subject to the supervision of the courts and the informational tribunal enforcement takes place through civil and criminal penalties which are applicable to data controllers, company directors, and company employees. Enforcement also takes place through enforcement, assessment, and failure to comply notices.

a. Information Commissioner:

The Privacy Commissioner's office is an independent body that has the ability to:

- Serve information notices requiring organizations to provide specified information within a certain time period for the purpose of determining whether or not they are complying with data protection principles.[61]
- Serve enforcement notices requiring organizations to take (or refrain from taking) specified steps in order to ensure they comply with the law.[62]
- Serve assessment notices to public or specified organizations and bodies. An assessment notice requires that the data controller allows the commissioner to enter into specified premises, direct the commissioner to documents, provides assistance to copies of documents to the commissioner, allows the

commissioner to inspect documents and equipments, etc., allows the commissioner to observe the processing of any personal data that takes place on the premises.[63]

- Serve assessment notices to conduct compulsory audits to assess whether organizations processing of personal data follow good practice.[64]
- If personal data is not being processed for the special purposes the commissioner may make a determination that will be issued to the data controller.[65]
- Submitting proposals for the notification of regulations to the secretary of the state.[66]
- Prepare a code of practice for the sharing of personal data.[67]
- Assist in cases involving processing for special purposes.[68]
- Inspect personal data recorded in specified international information systems.[69]
- Serve monetary penalty notices to the data controller. Before the commissioner can serve the monetary penalty notice, he must first indicate his intent to do so to the organization. The commissioner is responsible for determining and publishing a guide as to when monetary penalties will be served.[70]
- Inspect and enter a premise if granted a warrant by a circuit judge.[71]

b. Data controller:
The data controller determines the purposes for which and the manner in which any personal data are, or are to be processed, for example, an employer. Data controllers have the following responsibilities:

- Registering with the commissioner before processing any personal data[72] Failure to register is considered to be an offence.[73]
- Issuing notification to the commissioner of possible breaches in processing of data.
- Appointing data protection supervisors.[74]
- Putting in place adequate technical and organizational measures to safeguard personal data, which they are processing from destruction, adequate loss, unauthorized access or disclosure.

c. The Tribunal:

The information tribunal may make provision for:

- Securing the production of material used for the processing of personal data
- Inspecting, examining, operating, and testing equipment or material used in connection to the processing of personal data

Compensation: An individual is entitled to compensation from a data controller for damages caused from non-compliance by the controller.[75]

Offences: A person who fails to comply with an enforcement notice, information notice, or special information notice will be held criminally liable for the offence.[76] A person has the right to appeal to the tribunal against the notice.[77]

European Union

Proposal for the Directive of the European Parliament

.[78] The EU privacy regime consists of six different authorities and roles that are responsible for the enforcement of the Directive.

1. The EU Privacy Commission: Has been given implementing powers of the directive and the power to adopt relevant Acts.[79] This includes:
    - Developing effective international co-operation mechanisms to facilitate international co-operation for the protection of personal data[80]
    - Establishing standards for notification to be issued to the supervisory authority.[81]
    - Determining whether or not a third country has an adequate level of data protection
2. The European Data Protection Board: Advises the commission on any issue related to the protection of personal data in the Union, this includes:
    - Examining any question covering the application of the provisions, best practices etc. Reviewing the application of guidelines, recommendations and best practices, etc.
    - Providing the commission with an opinion on the level of protection enforced by third countries or international organizations
    - Promoting the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities
    - Promoting common training programmes and facilitating personnel exchanges between supervisory authorities
    - Promoting the exchange of knowledge and documentation with data protection supervisory authorities worldwide.[82]
3. Member States: Are responsible for carrying out and instituting the provisions of the Act in each respective state. This includes:
    - Laying down the rules and implementing suitable penalties[83]
    - Appointing one or more supervisory authorities.[84]
    - Ensuring that data controllers follow and adhere to laid out standards[85]
4. The Supervisory Authority: Is established by each member state. Every supervisory authority in the EU has the same duties and powers which include:
    a. Powers
        - Investigative powers
        - Powers of intervention
        - Ordering the restriction, erasure or destruction of data
        - Imposing a temporary or definitive ban on processing
        - Warning the controller
        - Referring a violation to national parliaments
        - The power to engage in legal proceedings where the provisions adopted

pursuant to this directive have been infringed upon or bring this infringement to the attention of the judicial authorities.[86]

- The power to engage in legal proceedings and bring an action to court in order to enforce the provision of the directive or to ensure consistency of the protection of personal data.[87]

b. Duties:

- Monitor and ensure application of the directive
- Hear and investigate complaints lodged by data subject or based on own initiative
- Check the lawfulness of data processing
- Provide assistance to other supervisory authorities to ensure consistent application of provisions
- Monitor the development of information and communication technologies and how they impact the protection of personal data
- Consult with member state institutions and bodies on legislative and administrative measures relating to the protection of individual's rights and freedoms
- Is consulted on processing operations
- Participates in on the European Data Protection Board
- Promotes awareness of privacy standards, etc
- Advises or request data subjects in exercising the rights laid down in provisions.

5. Controller and Processor: The controller is appointed by the member state. When processing is carried out on behalf of the controller, the controller must choose a processor – and be legally binded to that controller which acts only on instructions from the controller.[88] The controller and processor are responsible for:

- Implementing appropriate technical and organizational measures to ensure that processing of personal data is in compliance with the provisions.[89]
- Consulting with the supervisory authority before processing specific types and categories of data.[90]
- Documenting all processing systems under their responsibility and providing all information to the supervisory authority so that it can perform its duties.[91]
- Ensuring that any person under their authority only processes data where required by the Union or Member State Law.[92]

6. The Data Protection Officer: Is entrusted and appointed by the controller or the processor to:

- Inform and advise the controller or the processor of their obligations in accordance with the provisions of the directive.

- Monitor the implementation and application of the policies in relation to the protection of personal data.
- Monitor the documentation, notification, and communication of personal data breaches.
- Monitor the application for prior consultation to the supervisory authority.
- Monitor the response to requests from the supervisory authority.
- Act as the point of contact for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on the data protection officer's own initiative.[93]

7. The individual: The individual has a number of rights under the directive. Pertaining to the enforcement of the Act, if the supervisory authority does not respond to the individual within three months on the progress of a complaint, the individual has the right to judicial remedy.[94] The individual also has the right to a judicial remedy if they consider that their rights have been infringed upon in non-compliance with these provisions.[95] The individual has the right to receive compensation from the controller or the processor for the damage suffered.[96] The individual has the right to request from the supervisory authority that the processing is lawful.[97]

    - Remedies: The individual has the right to a judicial remedy against a controller/processor[98], or supervisory authority, specifically the individual has the right to bring a court action for obliging the supervisory authority to act on a complaint.[99]
    - Penalties: Penalties can be imposed on any natural or legal person, and should be implemented by member states.[100]
    - Compensation: Damage suffered by an individual should be compensated by the controller or processor.[101]
    - Complaints: Any individual or body, organization, or association which aims to protect the rights and interests of data subjects in relation to the protection of their data may file independently or on behalf of a data subject and complaint with the supervisory authority.[102]

United States

In the United States, the Federal Trade Commission (FTC) is the body responsible for overseeing and enforcing various privacy legislations.

1. *The Federal Trade Commission Act* gives the FTC a number of powers including:
    a. prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce.[103]
    b. investigate complaints and issue binding cease and desist orders.[104]
    c. issue civil penalties for non-compliance[105]
    d. investigative powers[106]
    e. require reports from persons, organizations, or corporations.[107]

In 2006 the US Safeweb Act was passed with the aim of addressing issues such as spyware, security breaches, malware etc. which facilitates increased cooperation with foreign law enforcement authorities and the FTC through confidential information sharing, and provision of investigative assistance.[108]

Canada

Personal Information and Electronics Act & the Privacy Act 1985

The Canadian Privacy Regime consists of two federal statutes and the office of the Federal Privacy Commissioner. Privacy Commissioners also exist at provincial and territory levels.

The Federal Privacy Commissioner has the power to:

- Receive and investigate a complaint filed by an individual. Before investigating a complaint the commissioner must inform the head of the government institution.[109] Individuals and government bodies are permitted to make representations in front of the commissioner.[110]
- Independently investigate and make recommendations with respect to complaints. This includes:
    a. the rights to summon and enforce the appearance of witnesses
    b. compel witnesses to give evidence or produce documents
    c. enter premises of government institutions and inspect records.
    d. access any document under the control of a government institution.
    e. the commissioner may recommend that the government institution takes corrective action.
    f. if the government institution does not follow the commissioner's recommendation to disclose information, either the complainant or the commissioner may apply to the Federal Court for review of the institution's decisions.[111]
- The commissioner is empowered to audit government institutions and recommend changes to effect compliance and report failures to comply with the institution and Parliament.[112]
- The commissioner may also assess whether a government institution's decision to designate a data bank as exempt from disclosure was correct, and has the ability to ask the Federal Court to rule on the question if the government institution fails to accept the commissioner's determination that it was not.[113]
- The commissioner must also submit annual reports to Parliament and may in addition submit special reports with respect to urgent matters.
- The commissioner oversees the application of privacy norms across the private sector.
- Conduct public educational programs, undertaking and publishing research, and encouraging organizations to develop compliance policies.

- The Privacy Commissioner may consult with provincial authorities to ensure that personal information is protected in as consistent a manner as possible.

---

1. The Consumer Protection Act, 1986, s. 2 V(d).
2. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, http://bit.ly/Q4sa6a
3. See http://bit.ly/OaojDf.
4. Sections 73, 74 and 75 of the Indian Contract Act, 1872 that deal with the monetary compensations for breach of contract includes not just individuals but also corporate, government departments, etc. See K.C. Skaria vs The Govt. of State of Kerala & Anr decided by Supreme Court of India, January 10, 2006, http://bit.ly/TVSGlU
5. Indian Contract Act, 1872, s. 10.
6. Indian Contract Act, 1872, s.13.
7. Indian Contract Act, 1872, s. 14.
8. Indian Contract Act, 1872, s.16
9. Indian Contract Act, 1872, s.17
10. Indian Contract Act, 1872, s. 18.
11. Indian Contract Act, 1872, s. 7.
12. Indian Contract Act, 1872, ss.14-20.
13. Indian Contract Act, 1872, s. 62.
14. Indian Contract Act, 1872, s. 72.
15. Indian Contract Act, 1872, s. 73.
16. Indian Contract Act, 1872, s. 74.
17. Indian Contract Act, 1872, s. 132.
18. Indian Contract Act, 1872, s. 142, 143.
19. Indian Contract Act, 1872, s. 133 a.
20. Indian Contract Act, 1872, s. 160.
21. Indian Contract Act, 1872, s. 196.
22. Section 20 of CPC deals with cause of action.
23. See http://bit.ly/MXhTXK
24. Zee Telefilms vs. Sundial Communications 2003, http://bit.ly/PLGfHH
25. Zee Telefilms vs. Sundial Communications 2003, paragraph 19.
26. Zee Telefilms vs. Sundial Communications 2003, paragraph 9.
27. Mr. Diljeet Titus, Advocate vs. Mr. Alfred A. Adebare 2006, http://bit.ly/Pgn2eQ
28. Mr. Diljeet Titus, Advocate vs. Mr. Alfred A. Adebare 2006, paragraph 50.
29. Mr. Diljeet Titus, Advocate vs. Mr. Alfred A. Adebare 2006, paragraph 54.
30. The Advocates Act 1961, chapter V, http://bit.ly/NKfIwf
31. DSCI Privacy Framework, http://bit.ly/Q8glQ1
32. Citizen Consumer and Civic Action Group, http://bit.ly/RIRUdN
33. See http://bit.ly/P78m5U
34. See http://bit.ly/O5qgW6
35. See http://bit.ly/OzS8iK
36. See http://bit.ly/Jj6xue
37. See http://bit.ly/SvdEHz
38. India Times Privacy Policy, http://bit.ly/Qxmh0q
39. CIBIL Terms and Conditions, http://bit.ly/QxU9JM
40. Ibid. PubMatic Privacy Policy, http://bit.ly/PBUzmw
41. Ibid. PubMatic Privacy Policy, http://bit.ly/PBUzmw
42. Brian Pereira, "Indian Data Centres Go 'Active-Active", *Information Week*, July 2, 2012, http://bit.ly/N7U9W0 (last accessed on July 5, 2012).
43. Reliance Communications Data Centers, http://bit.ly/PgnVEa
44. See http://bit.ly/8YFiRC
45. See list of State and Territory Acts: http://bit.ly/nia6xm
46. Australian Privacy Act, 1988, s. 27 (h).
47. Australian Privacy Act, 1988, ss.27 1(aa), (ad), (ae (b)).

48. Australian Privacy Act, 1988, s. 27 (1)(a).
49. Australian Privacy Act, 1988, s. 30 (1).
50. Australian Privacy Act, 1988, s. 50.
51. Australian Privacy Act, 1988, ss. 43-47.
52. Australian Privacy Act, 1988, ss. 71-72.
53. Australian Privacy Act, 1988, s. 27 1(c- e).
54. Australian Privacy Act, 1988, s. 27 1(f).
55. Australian Privacy Act, 1988, s. 27 (g).
56. Australian Privacy Act, 1988, s. 27 (j).
57. Australian Privacy Act, 1988, s. 27 (k).
58. Australian Privacy Act, 1988, s. 27 (p).
59. Australian Privacy Act, 1988, s. 27 (r).
60. Australian Privacy Act, 1988, ss.28-29.
61. UK Privacy Act, s. 43.
62. UK Privacy Act, s. 40.
63. UK Privacy Act, s. 42.
64. UK Privacy Act, s. 22.
65. UK Privacy Act, s. 45.
66. UK Privacy Act, s. 25.
67. UK Privacy Act, s. 52.
68. UK Privacy Act, s. 53.
69. UK Privacy Act, s. 54.
70. UK Privacy Act, s. 55.
71. UK Privacy Act, sch. 9.
72. UK Privacy Act, s. 17.
73. UK Privacy Act, s. 21.
74. UK Privacy Act, s. 23.
75. UK Privacy Act, s. 13 (1).
76. UK Privacy Act, s. 47.
77. UK Privacy Act, s. 47.
78. Article 2.
79. Sections 66 & 67.
80. Article 38.
81.. Article 28.
82. Section 49.
83. Article 55.
84. Article 42 (a).
85. Article 37.
86. Section 46.
87. Section 53.
88. Article 21.
89. Article 18.
90. Article 26.
91. Articles 23 and 25.
92. Article 22.
93. Article 32.
94. Section 51 (2).
95. Section 52.
96. Article 54.
97. Section 35.
98. Article 52.
99. Article 51.
100. Article 65.
101. Section 64.
102. Section 61.
103. FTC Act, s.45 (a).

104. FTC Act, s.45 (b)(f)(g).
105. FTC Act, s.45 (l).
106. FTC Act, s. 46(a).
107. FTC Act, s. 46(b).
108. See http://1.usa.gov/NpJzEn
109. Canada Privacy Act, s. 31.
110. Canada Privacy Act, s. 32.
111. Canada Privacy Act, ss. 29 -34.
112. Canada Privacy Act, s. 37.
113. Canada Privacy Act, s. 36.