INDIALAW

LAW

Privacy and Law

AUTHOR Appurv Bhatia

PUBLISHED 28 August 2014

By Srinivas Atreya Chatti

Introduction

"Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is." [1]

When we contemplate an invasion of privacy such as having our personal information gathered by companies in databases, we instinctively recoil. Most discussions on privacy appeal to people's fears and anxieties. However, what commentators often fail to do, is translate those instincts into a reasoned, well-articulated account of why privacy problems are harmful. When people claim that privacy should be protected, it is unclear precisely what they mean. This lack of clarity creates a difficulty for policy making or resolving cases because lawmakers, enforcement agencies and judges cannot easily articulate the privacy harm. The interests on the other side including free speech, efficient consumer transactions and security-–are often much more readily articulated. Therefore, courts and policymakers frequently struggle in recognizing privacy interests and when this occurs, cases are dismissed or laws are not passed. The result is that privacy is not balanced against countervailing interests.[2]

What is Privacy?

While it is tempting to engage in an etymological inquiry of the definition of privacy, it would be a rather futile exercise because practically, privacy cannot be understood independently from society. As sociologist Barrington Moore Jr. aptly observes, "the need for privacy is a socially created needandwithout society there would be no need for privacy." Perhaps the most symbolic definition of privacy is simply 'the right to be left alone', but this definition too turns out to be rather inadequatewhen the everyday realities of the information age are factored in. One can also argue that privacy is the relief from a range of kinds of social friction. However, privacy is not freedom from all forms of social friction but rather, it is protection from a cluster of related activities that impinge upon people in related ways. These activities often are not inherently problematic or harmful and more that often the element of consent forms the pivot whether an activity is violative of one's privacy.

Why is Privacy Relevant?

Privacy as a matter of subjective as well as objective interest has pervaded public debate over the recent past for a variety of causes and reasons but which can be largely traced to the growth and development of electronic communications. A brief inquiry into the practical implications on the right to privacy in the digital age reveals the vast many of threats. Threats to privacy arise over a large spectrum of sectors ranging from law enforcement and national security to data protection and biometrics. Very broadly,one hand, there is real and direct threat to an individual's privacy from surveillance both private (which is illegal) and state sponsored (which remains legal).

On the other hand, while Information and Communications Technologies (ICTs) have greatly enhanced our capacities to collect, store, process and communicate information, the rapid increase in the adoption and use of Information Communication Technologies platforms has also revealed a host of issues ranging from protection of commercial and financial data to protecting one's online identity. Firstly, data on personal computers can be compromised with consequences ranging from personal embarrassment to financial loss. Secondly, transmission of data over the Internet and mobile networks is equally fraught with the risk of interception, both lawful and unlawful, which could compromise our privacy. Thirdly, in the age of cloud computing when much of "our" data – emails, chat logs, personal profiles, bank statements, etc., reside on distant servers of the companies whose services we use, privacy becomes only as strong as these companies internal electronic security systems. Fourthly, the privacy of children, women and minorities tend to be especially fragile in this digital age and they have become frequent targets of exploitation. Fifthly, The internet has spawned new kinds of annoyances from electronic voyeurism to spam or offensive email to 'phishing' – impersonating someone else's identity for financial gain, each of which have the effect of impinging on one's privacy.[3]

In particular, the right to privacy of a citizen against the state has become a subject of concern and intense debate in the public field as a result of growing evidence of increased state-sponsored surveillance in countries across the world including 'democracies' like the United States of America (NSA's PRISM) and India (CMS). It is a confirmed fearthat the explosion of digital communications content and information about communications (known as communications metadata), coupled with decreasing costs of storing and mining large sets of data and the provision of personal content through third party service providers make state surveillance possible at an unprecedented scale. Communications surveillance in the modern environment encompasses the monitoring, interception, collection, preservation, retention, interference, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future.[4] Reports of the extensive use of dragnet technologies and other clandestine operations by state agencies under the pretence of national security has set alarm bells

ringing across the public domain andseveral crucial questions regarding the legality and ethics and more importantly the efficacy of such operations remain unanswered.

Further, there are concerns with privacy and autonomy issues regarding the collecting and aggregation of private or personal information both by the state as well as internet companies and service providers. Massive data collection initiatives of the state like the UID, NATGRID, CCTNS etc.involve collection and storage of vast amounts of sensitive data of people in data centres. More worrying is the lack of an adequate security framework for protection of this data. On the other hand, service providers including telecom operators or social media platforms also handle large amounts of personal information and data which are liable to be breached or exposed if adequate security measures are not taken. Adding to this is the growing threat of cyber-terrorism and information warfare.

Therefore, the causes and solutions to these issues have multiple dimensions and facets and legal or administrative fixes are not always sufficient. Apart from strengthening the legal structures,a socio-technological approach to these issues is warranted.

Concept of Privacy

Although various attempts at explicating the meaning of “privacy” have been made, few have attempted to identify privacy problems in a comprehensive and concrete manner. The modern contours of the tort of privacy can be traced back to the seminal article The Right to Privacy[5] which seized upon the metaphor of ‘man’s house as his castle’ to call for a common law right to privacy. A more comprehensive attempt was undertaken in 1960 by the legendary torts scholar William Prosser and he discerned four types of harmful activities redressed under the rubric of privacy:

- Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
- Public disclosure of embarrassing private facts about the plaintiff.
- Publicity which places the plaintiff in a false light in the public eye.
- Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.

The concept of privacy has however evolved through into the information age and a modern taxonomy of privacy[6] devised by Daniel Soloveis founded on the premise that the state of privacy law today is in disarray. The objective of the article is to codify and make sense of the harms caused by a breach of privacy in the present era. Privacy harms have been categorized into four distinct categories namely information collection, information processing, information dissemination and invasion.

The first group of activities that affect privacy involves information collection which includes Surveillance and Interrogation. The second group of activities involves the way information is stored, manipulated, and used and is collectively referred to as “information processing.” The third group of activities involves the dissemination of information which includes aspect of Breach of confidentiality, Disclosure, Exposure, Increased Accessibility; Blackmail is the threat to disclose personal information. Appropriation involves the use of the data subject’s identity to serve the aims and interests of another. Distortion consists of the dissemination of false or misleading information about individuals. Information Dissemination activities all involve the spreading or transfer of personal data or the threat to do so. The fourth and final group of activities involves invasions into people’s private affairs. Invasion, unlike the other groupings, need not involve personal information (although in numerous instances, it does). Intrusion concerns invasive acts that disturb one’s tranquillity or solitude. Decisional interference involves the government’s incursion into the data subject’s decisions regarding her private affairs.

Right to Privacy

It is commonly believed that Indians do not place much value on individual autonomy. Although the latter has begun to enter Indian life and exercises varying degrees of influence on different sections of society and in different areas, its reach remains rather limited and its impact uneven.[7]

In spite of this notion, considerable questions have been raised regarding privacy infringements before courts and the law of privacy in India has been largely developed through precedent.[8] Alleged breaches of privacy and complaints of unwanted state intrusion have been examined by the courts over the decades and the right to privacy has been sustained by expanding the scope of right to life and liberty under Article 21 of the Indian Constitution.

The judgments in *Kharak Singh v. State of Uttar Pradesh* [9] and *Gobind v. State of Madhya Pradesh* [10] are of significance in this regard. The 1997 case of *PUCL v. Union of India* [11] is also significant regarding state intrusions and right to privacy as the Courtset out procedural safeguards which would have to be followed for wiretapping under the Indian Telegraph Act. Further, the concern of right to privacy has intermittently but certainly been stretched beyond breaches by the state and Courts have over the years examined and expounded on issues like the right to privacy of medical records of patients[12], the conflict between right to

privacy and free speech[13] and more recently, privacy in the context of sexual identities[14].

In spite of this limited judicial oversight, it is but a fact that there is still limited protection for the right to privacy as India does not currently have a sui-generis statute that safeguards privacy horizontally across different contexts.[15] However various statutes dealing with issues as diverse as banking and finance, professional ethics of lawyers, doctors and chartered accountants, information technology and telephony contain provisions which either explicitly or impliedly protect privacy or offer victim remedies for their breach.

Law of Privacy

The Information Technology Act, 2000 which is of much relevance today contains a number of provisions which are intended to safeguard against online/computer related privacy. The Act provides for civil and criminal liability with respect to hacking (Sections 43 & 66) and imprisonment of up to three years with fine for electronic voyeurism (Sec. 66E), phishing and identity theft (66C/66D) or sendingoffensive emails (Sec. 66A) etc.

On the flipside, Section 69 is titled the “power to issue directions for interception or monitoring or decryption of any information through any computer resource.” This section is perhaps the legal basis for all the latest state sponsored surveillance activities that may be undertaken in the pretext of intelligence gathering and national security including the Central Monitoring System. The section mirrors section 5(2) of the Telegraph Act, containing the same limitations on the exercise of the power to issue directions. It contains a similar structure adhering to the constitutional limitations as prescribed in PUCL v. Union of India judgment, where the direction may only be issued when a public emergencyor a public safetysituation exists. It also contains the requirement of recording reasons for issuing the direction and mentioning the 5 classes of events as contained in section 5(2). It however does not cause surprise that the recent regulations prescribed under section 69(2) for providing the procedure for issuing directions also broadly follow Rule 419-A of the archaic Indian Telegraph Act. The fact that the present laws mirror most of the procedural safeguards of documentary adherence, oversight and automatic expiry of an older, archaic law reflect the apathetic approach of the state in preserving the right to privacy of its subjects.

Data Protection and Law

The overall scheme of the law relating data protection in India is structured under the provisions of the Information Technology Act and is a rather recent development. Contextually,the data protection regime in India is direct result of the development of information technology industry with Indian companies playing a major role in the global outsourcing business. Over the past decade, it was perceived that the lack of a proper data protection regime would adversely impact upon the flow of outsourcing business from European Union countries and concerns were raised that this lacunae might divert outsourcing business within the European Union to the new Eastern European member states, or to other countries that provided adequate levels of protection for personal data via legislative or other means.Therefore, it can be safely assumed that the importation of personal data from EU countries thus appears to be the driving force behind the Indian data protection debate, and earlier attempts to introduce data protection legislation.[16]

The Information Technology Act, 2000was therefore amended and specifically, Section 43A was introduced in 2008 which made a start at introducing a mandatory data protection regime in India. The provision obliges corporate bodies who ‘possess, deal or handle’ any ‘sensitive personal data to implement and maintain ‘reasonable security practices’, failing which, they would be liable to compensate those affected by any negligence attributable to this failure. In addition to this, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 were subsequently notified and the Rules lay down more comprehensive guidelines regarding data privacy.

There are three key aspects of the Act and Rules that bear highlighting. Firstly, the Act and Rules cater to three groups namely Body Corporates, Information Providers (or Data subjects) and the Government. These rules address the:

1. Obligation of the corporates who collect the sensitive personal data of an individual – the obligations being those pertaining to its use and disclosure.
2. The rights of the information provider, with a view to curb indiscriminate disclosure of such information without the consent of the data subject.
3. The right of the Government to access sensitive personal data of individuals in cases of investigation, etc.

The second aspect is the definition of ‘Sensitive personal data or information” which is defined as any information that the Central Government may designate as such, when it sees fit to. By definition, Sensitive Data includes within its ambit the following types of information:

1. Passwords
2. Financial information such as Bank account or credit card or debit card or other payment instrument details ;
3. Physical, physiological and mental health condition;
4. Sexual orientation; medical records and history;
5. Biometric information;
6. Any detail relating to the above clauses as provided to body corporate for providing service; and
7. Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:
8. Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

While the definition of sensitive personal data appears and attempts to be comprehensive, it has in fact been observed to be of a broad character and it can be interpreted to include, within its ambit, a wide array of information. In this aspect, it is essential to determine a precise definition of 'sensitive personal information' because broad interpretation will add to the ambiguity of the scope of not only these Rules but also of Section 43A. Thus, it seems to follow that, any ambiguity in the definition, fails to serve the very purpose of the Rules, to begin with, since the whole enactment deals with the concept of processing of 'Sensitive Personal Data or Information'. In order for this provision to be clearer, the definition could be amended to include inter alia, 'information which is capable of personally identifying a person, individually or when aggregated'.[17] Another aspect that the present laws fails to distinguish is between two distinct types of data namely personal data and sensitive personal data as the processing of sensitive personal data must be subject to conditions that are stricter than those applied to personal data.

Thirdly, the 'reasonable security practices' which the Act obliges body corporate to observe are restricted to such measures as may be specified either 'in an agreement between the parties' or in any law in force or as prescribed by the Central Government. However, the Rules provide that in the absence of such agreement 'reasonable security practices and procedures' to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the Central Government.

In practice, data controllers are obligated to formulate a privacy policy for handling or dealing with personal information and sensitive personal information. The policy must be available to be viewed by the data subjects who provide information under a lawful contract and must include the following aspects.

1. Clear and easily accessible statements of the data controller's practices and policies;
2. The type of personal information or sensitive personal information that may be collected;
3. The purpose of collection and use of the information;
4. Conditions of disclosure of information; and
5. Reasonable security practices and procedures implemented to ensure confidentiality of information.[18]

Another important facet of data protection is the guidelines concerned withcollection of information and retention of data which fundamentally involve concept of consent.Rule 5 of the Rules deals with the collection of sensitive personal data or information and it states inter alia that a body corporate has to first obtain consent in writing through letter, fax or email, from the provider of such information, regarding purpose of usage, before collection of such information. This rule is conterminous with Article 7 of the EU Directive[19], which reflects the same principle as it states that personal data may be processed only if the data subject has unambiguously given his consent to the same. Further, Rule 5 gives 'the provider of information' certain privileges of modifying such information as and when necessary and withdrawing the consent given earlier. Therefore, data controllers must obtain the data subject's consent regarding the purpose of use, before collecting any sensitive personal information and no sensitive personal information must be collected unless the information is collected for a lawful purpose and is connected with a function or activity of the data controller and which is considered necessary for that purpose.

Data controllers must also not retain sensitive personal information for a period longer than it is required for fulfilling the purposes for which the information is collected or as may be required by law. Data collectors must also obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or in any other country that ensures the same level of data protection as provided for under Rules. However, consent is not necessary for the transfer if it is required for the performance of a lawful contract between the corporate entity and the provider of information or as otherwise specified in the Act.[20]

Another pertinent aspect is thatcollectors of information must also provide an option to the data subjects not to provide the data or information sought to be collected. Data subjects also should have an option of withdrawing consent given for use of sensitive personal information. However, the rules fail to clearly distinguish between 'the provider of information' and 'individual to whom the data pertains' which gives rise to a lot of uncertainty on a prima facie reading of the rules.[21]

Rule 6 deals with disclosure of information and it states that prior permission of the provider of information has to be obtained before any disclosure is made to a third party and any third party receiving such information is not entitled to disclose it further unless the disclosure has been already agreed to in the contract between the data subjects and the data controllers or disclosure is necessary for compliance with a legal obligation.The exception to this rule is where either disclosure must be made to government agencies mandated under law to obtain information for the purposes ofverification of identity, prevention, detection and investigation of crimes, or prosecution or punishment of offences, or an order under law (such as a court order) has been made.

The Information Technology Act also prescribes penalties and punishments for contraventions of the Act. For instance, disclosure by the government of information obtained in the course of exercising its interception powers under the Act is punishable with imprisonment of up to two years and fine(Sec. 72). Section 72A of the Act penalizes the unauthorized disclosure of "personal information" by any person who has obtained such information while providing services under a lawful contract. Such disclosure must be made with the intent of causing wrongful loss or obtaining a wrongful gain and is punishable with imprisonment which may extend to 3 years or a fine of Rs.500,000 or both.

There is however growing dissatisfaction over the present framework for data protection created under S. 43A and corresponding Rules. The information services industry in India is heavily reliant on strong data protection measures yet data transfers to India continue to occur on the strength of contractual data protection requirements. Adequate protection standards (for incoming European data) are secured primarily by incorporation of the Standard Contractual Clauses within the binding terms of the data transfer contract. Compared to the EU data protection directives, the India data protection regimeis limited and definitively not sufficient to ensure adequate protection. In that sense, Regulations issued by the RBI contain more certain provisions containing data protection but are limited in scope. There is therefore an impending need to revamp the existing law and develop a more comprehensive regime which is on par with the EU data protection regime.

Privacy Legislation: Imperative Need

The commoditization of information has had large scale socio-political and economic implications in the last decade and prevailing issues of privacy extend beyond commonly perceived causes. The initiation of national programmes like Unique Identification Number (UID), National Intelligence Grid (NATGRID), Crime and Criminal Tracking Network System(CCTNS), DNA Profiling, Reproductive rights of Women, Privileged Communications and Brain Mapping, most of which will be implemented through ICT platforms, have increased collection of citizen information by the government and serious concerns have emerged on their impact on the privacy of persons. The lack of an overarching policy governing the collection of information by the government or other private has led to ambiguity over who is allowed to collect data, what data can be collected, what are the rights of the individual, and how the right to privacy will be protected.Moreover, the extent of personal information being held by various service providers, and especially the enhanced potential for convergence that digitization carries with it is a matter that raises issues about privacy.[23]

It is under these considerations that the Justice AP Shah Report on Privacy is of much relevance today. The report envisages a five point framework encompassing technological neutrality and inter-operability with international standards on multi-dimensional privacy issues in like surveillance, collection of DNA, physical privacy, horizontal applicability between the government and private sector, conformity with certain privacy principles and establishment of a co–regulatory enforcement regime. The report in its recommendations also proposes a framework for a Privacy Act which is intended to establish clear boundaries and clarify definitions and harmonise legislations, policy, and practices over a vast array of issues[24]. The Act also articulates an enforcement regime including establishing the office of the Privacy Commissioner at the regional and central levels, defining the role of self regulatory organizations and co-regulation, and creating a system of complaints and redressal for aggrieved individuals. The Act could also prescribe safeguards for physical privacy including search and seizure and enumerate offences, associated remedies, and penalties. The report address issues of growing relevance and is an important step forward in strengthening the law on privacy.

[1] *Judith Jarvis Thomson, Philosophy & Public Affairs, Vol. 4, No. 4 (Summer, 1975), pp. 295-314*

[2] *Daniel Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review*

[3] *Prashant Iyengar, Privacy and the Information Technology Act — do we have the Safeguards for Electronic Privacy?*

[4] *International Principles on the Application of Human Rights to Communications Surveillance available at*

[5] *Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 197 (1890)*

[6] *Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477, 482-483 (2006)*

[7] *Bhikhu Parekh, Private and Public Spheres in India, 12 Critical Rev. Int'l Soc. & Pol. Phil. 313, 317 (2009)*

[8] *Apar Gupta, Balancing Online Privacy in India, Indian Journal of Law and Technology, Vol 6 (2010)*

[9] *AIR 1963 SC 1295 (SubhaRao, J., dissenting) (concerned a challenge to the constitutionality of Rule 236 of the U.P. Police Regulations)*

[10] *(1975) 2 SCC 148 (Per K. K. Mathew, J. et al.) (holding that unnecessary domiciliary visits and picketing were a breach of the petitioner's right to privacy)*

[11] *(1997) 1 SCC 30*

[12] *Mr. 'X' v. Hospital 'Z', AIR 1999 SC 495*

[13] *R. Rajagopal v. State of Tamil Nadu,(1994 SCC (6) 632)*

[14] *Naz Foundation v. Union of India,WP No. 7555 of 2011*

[15] *Privacy in the Developing World, IDRC*

[16] *R Ananthapur, "India's new Data Protection Legislation", (2011) 8:2 SCRIPTed 192*

[17] *Apar Gupta,2011, Comments on Draft Sensitive Personal Information Rules*

[18] *External Link*

[19] *Directive 95/46/EC*

[20] *Data Protection Laws of the World, DLA Piper*

[21] *Radha Raghavan and Ramya Ramchandran , Data Protection Law in India: An Overview*

[22] *Comparison of International Privacy Principles, Report of The Group of Experts on Privacy 2012, Planning Commission, Government of India*

[23] *Ibid*

[24] *Interception, the use of personal identifiers, the use of audio and video recordings, the use of bodily and gene-material, and the use of personal information by the government and the private sector*