PRESERVING CONSTITUTIVE VALUES IN THE MODERN PANOPTICON: THE CASE FOR LEGISLATING TOWARD A PRIVACY RIGHT IN INDIA

Ujwala Uppaluri & Varsha Shivanagowda[*]

As on date, the only meaningful, if arguably broad, affirmation of a right to privacy has been in the context of the Supreme Court's treatment of Art. 21 of the Constitution, which embodies the guarantee of a right to life and personal liberty. No substantial legislative measures granting and detailing a broad and general right of privacy presently exist in the Indian context, although some measures are scattered across context-specific legislation. Recent events have brought to light the need to operationalise these judicial observations through a legislative statement of the right fleshing out the field within which the sanctity of the private domain will be recognised and upheld. This paper seeks to explore the contours of the notion of a general right to privacy. It confronts the critiques of such a right and discusses the predominant working models in other major jurisdictions. In the result, it asserts the need for an umbrella legislation addressing the varied areas in which the right of the individual to privacy, against governmental incursion into private spaces as well as against other forms of intrusion by the media and other citizens, must accrue.

I. INTRODUCTION

Recent concens with privacy and autonomy issues in India have arisen with regard to the State's role in collecting and aggregating private or personal information in the context of the work of the Unique Identification Authority of India (UIDAI)[1] and the National Intelligence Grid (NATGRID).[2]

---

[*] 3rd and 2nd year students respectively, the W.B. National University of Juridical Sciences, Kolkata. We thank Malavika Jayaram for her advice and insights. Any errors remain our own.

[1] Press Trust of India, *UIDAI Gets First Data Misuse Complaint*, Times of India (New Delhi) October 3, 2011; Deva Prasad, *Analysing the Right to Privacy and Dignity with Respect to the UID*, available at http://www.cis-india.org/internet-governance/blog/privacy/privacy-uiddevaprasad (Last visited on October 30, 2011); Binu Karunakaran, *India's UID and the Fantasy of Dataveillance*, available at http://www.countercurrents.org/karun240809.htm (Last visited on October 30, 2011).

[2] *See, e.g.* Vinay Kumar, *Cabinet Panel Clears National Intelligence Grid*, The Hindu (New Delhi) June 6, 2011; *National Security and Privacy: Civil Liberties are not Getting the Needed Attention*, Business Standard (New Delhi) May 27, 2011; PRS Blog, *NATGRID: Should Parliament have a role?*, available at http://www.prsindia.org/theprsblog/2011/06/20/natgrid-should-parliament-have-a-role/ (Last visited on October 30, 2011).

In addition, the role of non-state institutions and individuals in the erosion of the expectation of privacy in personal communications, as exemplified by the media by its recent publication of the contents of unauthorised phonetaps,[3] has also been the cause of considerable concern. While privacy rights have been addressed in a diffused and scattered manner under existing Indian laws,[4] as of the present, no single law attempts to cogently and comprehensively address questions relating to privacy and provide for safeguards with regard to them. The consequence, then, is that an injured party is not ordinarily able to assert the violation of a right that can be *explicitly* located on the statute books. While a derivative constitutional right has been read into Art. 21 of the Constitution judicially, these interpretations have been vague, and at best of limited use to any substantial evolution of the law on the point.

This paper attempts to undertake a preliminary enquiry into the tenability of a general law of privacy in India. It advances the argument for an umbrella privacy law for India as a solution to problems including those outlined above, in the following manner. Part-II of the paper highlights the particular problems that the search for a reasonably sound and legally appliable definition is mired in. It also attempts to suggest the way towards a pragmatic measure of definitional clarity. Part-III examines the philosophical and jurisprudential basis that the call for a recognition of privacy rights has rested upon, and emphasises the inherent, stand-alone value that is, and we contend must be, ascribed to a general privacy right. Part-IV foregrounds percieved challenges to the grant of a right to privacy and addresses them in turn to establish that the case for a legislative grant of the privacy protection is both theoretically sound and practically workable. Part-V then mentions the possible approaches to the realization of the privacy right and discusses their relative merits. Part-VI summarily outlines, as far as is relevant to the argument in this paper, the liberty and dignity models on which a scheme of privacy protection can be constructed. Parts VII and VIII undertake an enquiry into the state of the existing Indian law and the salient features of the Privacy Bill, 2011 in its current state, respectively. The paper finally concludes that the most recent legislative attempt at providing for a statutory right to privacy is a commendable one, given the growing need for a clear twofold legislative formulation of the individual's right to privacy and of the limits of the State's power of (justified) incursion into private spaces is necessary.

---

3 Elonnai Hickok, *Should Ratan Tata be Granted the Right to Privacy*, available at http://privacyindia.org/2010/12/07/should-ratan-tata-be-granted-the-right-to-privacy/ (Last visited on October 30, 2011); Maneesh Chhibber, *After Radia Tapes, Govt works on privacy law*, Indian Express (New Delhi) December 19, 2010; India Knowledge@Wharton, *The Tata Tapes and Beyond: Juggling Privacy, Reputation and Public Interest*, December 16, 2010, available at http://knowledge.wharton.upenn.edu/india/article.cfm?articleid=4555 (Last visited on October 30, 2011).

4 *See infra* Part-VII.

While this paper attempts to make a *general* case, in principle, for why it is both necessary and favourable to legislate towards preserving Indian citizens' privacy, and considers the question of how a horizontal application of the right to privacy will be achieved (between citizens *inter se*), where decisional privacy is located (in the context of reproductive autonomy or sexuality) and so on, the discussion emphasises the vertical application of privacy right (as between State and citizen) with regard to informational privacy in particular, in as much as the right does not exist even in its classical form (of restraining the limits of State power through surveillance and record-keeping) at present. On the understanding that the project of preserving privacy must begin at this level, especially since we locate privacy in Part-III of the Constitution whose Art. 12 makes the preservation of these rights the State's burden (although, with judicial evolution, not exclusively), this paper makes the first and preliminary arguments towards comprehensive privacy protections under Indian law.

II. PRIVACY: THE CONCEPT & THE DEFINITION PROBLEM

An historic dichotomy between public and private spheres can be located in the Aristotelian distinction between politics (*polis*) and the domestic, familial space (*oikos*) that existed in classical Athenian society.[5] This disctinction has persisted, with the dichotomy being heightened and entrenched in modern and postmodern societies by the advent of an increasingly powerful and intrusive State entity, and of technological advances in particular. Early enquiries into cultures by scholars, chief among them Margaret Mead in cultural anthropology, have concluded that all societies reflect a concern for private spaces in their recognition of secrecy in ritual ceremonies and concealment, for example.[6] Notwithstanding the recognition of this distinction traditionally, the notion of privacy has remained a nebulous one, leading to charges that it is analytically unserviceable.[7] More fundamentally, in present times even this distinction is becoming increasingly difficult to maintain with the advent of technologies such as social networking and of the ubiquity of data sharing generally. The problem of definition arises out of these difficulties with delineating the scope and limits of the term. Lexically, it is "[t]he condition or state of being free from public attention to intrusion into or interference with one's acts or decisions"[8], and while it has been understood to be an area of concern to a range of disciplines, including moral philosophy, anthropology, sociology,

---

5 *See* J. Roy, *'Polis' and 'Oikos' in Classical Athens*, 46(1) Greece & Rome, 1 (1999). *See also* Edward Shils, *Privacy: Its Constitution & Vicissitudes*, 31 L. & Contemp. Probs 281, 283 (1966) and Jürgen Habermas, The Structural Transformation of the Public Sphere (Thomas Burger Trans., 1991).

6 Margaret Mead, Coming of Age in Samoa (1928).

7 Lee A. Bygrave, Data Protection Law: Approaching its Rationale, Logic and Limits 126 (2002).

8 Black's Law Dictionary (Bryan Garner, ed.) 1233 (2004).

law and public policy, no generally accepted definition of the term has emerged, whether in positive or negative terms.

The manner of its conception, its scope and limits have all been subject to disagreement. Related notions of intimacy, confidentiality and secrecy have, *inter alia*, led to disgreements over its content, and have raised the question of whether it consists of any independent and freestanding elements at all or whether it can be subsumed within rights already existing. Individuals are arguably entitled to their privacy rights as participants in a multiplicity of spheres: in society (real or virtual), as citizens, as consumers and so on. The term has been charged with being "protean"[9] and "lacking in clarity",[10] thus disallowing it from being of any real use to define and protect rights in the private sphere. Some have even gone as far as to suggest that the definition exercise is "ultimately futile".[11] An early definition posited by Warren and Brandeis in their seminal paper,[12] which casts privacy as a 'right to be let alone' has, in the same vein, been criticised for its overbreadth, notwithstanding the recognition that the formulation was indeed a meaningful one. Another infuential formulation of the privacy definition is that it is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[13] But even this limits privacy to informational control.[14]

Writers have focused instead on breaking down the term and its connotations. One useful approach to simplifying the definition problem is arguably to separate the descriptive content of the privacy right from its normative content, with the former describing the limits to which the protection actually extends (the 'is') and the latter making the case for what should be protected as private (the 'ought').[15] Another approach has been to distinguish between reductionist and anti-reductionist attempts to define the term. The reductionist approach refers, in Powers' formulation, to creating and applying a specific or narrow account of which invasions clearly include a loss of privacy while the anti-reductionist approach refers to taking a broader approach by which a wider range of interferences with persons and personal spaces are viewed as raising

---

9 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Penn. L. Rev. 477, 479 (2006).

10 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L. J. 1151, 1154 (2004).

11 Raymond Wacks, *The Poverty of "Privacy"*, 96 L. Q. Rev. 73, 76-77 (1980). *See also* Ken Gormley, *One Hundred Years of Privacy*, Wis. L. Rev. 1335 (1992) (Gormley concludes that the search for a definition is a "misguided quest").

12 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 205 (1890).

13 *See* Alan Westin, Privacy & Freedom 7 (1967).

14 *See* Louis Lusky, *Invasion of Privacy: A Clarification of Concepts*, 72 Colum. L. Rev. 693, 709 (1972) (Lusky records other instances of privacy defined in terms of information control).

15 Judith Warren DeCew, *Privacy*, available at http://plato.stanford.edu/entries/privacy/ (Last visited on September, 1, 2011).

the claim of a violation of privacy.[16] The argument is that adopting the former path in defining privacy will overcome the problem of terminological vagueness and allow the right to be legislatively operationalised.[17] Another particularly useful approach to constructing a coherent and legally workable privacy account has been through the pragmatic exercise of classifying activities that are seen as harmful to privacy interests.[18]

III. PRIVACY IN LEGAL AND MORAL PHILOSOPHY

Privacy should be and is generally recognized as intuitively important, even in the absence of an entirely visible or explicit philosophical justification.[19] A right of privacy, even in the absence of extraordinary situations of an interference with private spaces or information, has been recognised as being intrinsically valuable as an element governing, at a basic level, human interaction and relationships.[20] Although an individual sense of privacy is subjective, several instances of its common and shared recognition have by now entrenched themselves in modern societies, as for instance, through the provision for secret ballot in democracies and the right against arbitrary search and seizure.[21]

Though not explicitly present or treated in legal theory, privacy interests can be cogently located and justified in philosphical and jurisprudential thought. John Stuart Mill, in his impassioned argument for the restriction of governmental authority from particular domains which may (if at all) be subject only to informal self-regulation, espoused the notion of a protected private domain.[22] The common law tort of invasion of privacy is argued to be rooted in the premise that violations of rules granting privacy are violative of dignity and human personality.[23]

---

16 Madison Powers, *A Cognitive Access Definition of Privacy*, 15 Law and Philosophy 369 (1996).

17 *Id*.

18 *See, e.g.,* Solove, *supra*, note 9 (Solove's fourfold taxonomy of privacy harms is an instance of such a classification. Interestingly, it succeeds an earlier statement that privacy is not reducible to any unifying or "core" essence in Daniel J. Solove, *Conceptualizing Privacy,* 90 Cal. L. Rev. 1087, 1130 (2002).

19 Charles Fried, *Privacy*, 77 Yale L. J. 475 (1968).

20 James Rachels, *Why Privacy is Important*, 4 Philosophy And Public Affairs 323 (1975).

21 Alan P. Bates, *Privacy - A Useful Concept?*, 42 Social Forces 429 (1964).

22 *See* John Stuart Mill, On Liberty 12, 13, 74-75 (1859) (In particular, Mill contends that "a person's conduct affects the interests of no persons besides himself … there should be perfect freedom, legal and social, to do the action and stand the consequences").

23 Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Cal. L. Rev. 957 (1989) (Professor Post argues here that both values imbue the construction of a privacy tort.). *See also* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001).

One approach in the philosophy of privacy has been to cast it as an element of liberty, as in the United States. Another is to view it as an element of dignity, which finds favour in European privacy models. Arguably, a system of morality in which positive privacy rights are valued is essentially Kantian, with inherent value accruing to notions of dignity of the self. This affords the grounds for a deontological construction of the privacy right, *i.e.*, one based around the obligation to act in certain ways, rather than one which is focused on the results of an action. Privacy has also been recognised as an element necessary to the construction and maintenance of the autonomy of the self.[24] The Kantian paradigm's distinction between public and private is the result of an emphasis on individual autonomy.[25] Closely intertwined with essential Kantian notions of respect[26] and dignity, privacy is thus a concept of absolute and constitutive value and not merely instrumental value, being, as it is, fundamental also to love, frienship and trust.[27] Further, according to the Rawlsian thesis, in which the relevant question to ask must relate to what rational and reasonable individuals will acquiesce to and value in constructing society, States will attempt to secure equals rights to a fully adequate system of *basic* liberties, with the notion of liberty covering the range of basic and elemental individual interests that such a system will seek to protect.[28] Liberty and self-respect are both 'primary goods'[29] under this formulation.

Neo-naturalists, who take from and extend the reasoning of classical naturalists such as Thomas Aquinas or Blackstone and who share the starting premise that laws exist to facilitate the common good, also recognise life as the first basic value in a list of 'basic human goods', holding that it would include the right to cerebral and not merely bodily health.[30] Finnis also characterises practical reasonableness as a basic human value of complex content, covering within its sweep the effective freedom to allow the individual to choose his lifestyle and shape his character.[31] The right to life as constructed in qualified terms has found legal footing in constitutional texts and/or their interpretations. In India, the Supreme Court has held in *Francis Coralie Mullin* v. *Administrator, Union Territory of Delhi*[32] that the right to life necessarily means the right to a life of dignity. As a concomitant to the right to life, we

---

[24] Joseph Kupfer, *Privacy, Autonomy, and Self-Concept*, 24 American Philosophical Quarterly 81 (1987).

[25] Regulating the Global Information Society 55 (Christopher T. Marsden ed., 2005).

[26] Immanuel Kant, Critique of Practical Reason 76 (1956).

[27] *See* Fried, *supra* note 19.

[28] John Rawls, *The Sense of Justice*, 72 Phil. Rev. 281 (1963); John Rawls, *Justice as Fairness*, 67 Phil. Rev. 164 (1958) (This is the Liberty Principle).

[29] John Rawls, A Theory of Justice 92 (1971). (Rawls defines primary goods as "things which a rational man wants whatever else he wants". They are interests essential to the pursuit of the full range of conceptions of the good life and Rawls sees their provision as a fundamental concern of political institutions in all societies).

[30] John Finnis, Natural Law and Natural Rights 86 (1980).

[31] *Id.,* 88

[32] (1981) 1 SCC 608.

contend that there is a fair argument that can be made for the immanence of the right to privacy as well. Finnis also recognises that "[t]he modern language of rights provides...a supple and potentially precise instrument for sorting out and expressing the demands of justice".[33] His treatment of rights is predicated on the proposition that human rights are merely the "contemporary idiom" for these self-evident 'natural rights'.[34] We contend, on the strength of the above, that the right to privacy is of this character.

All of the above demonstrates that the value of the term is, therefore, considerably more than associative and a case can be made of privacy as a legal concept of intrinsic value, irreducible to other allegedly broader interests. In the result, we contend that privacy is a discrete right, capable of, and requiring, State protection.

IV. ADDRESSING THE COUNTERS TO THE PROVISION OF PRIVACY RIGHT

Even as the arguments outlined in the preceding section go some way in establishing that the attempt to recognise a separate right to privacy in the Indian context is a valuable undertaking, theoretical hurdles to the adoption of a privacy right do, however, exist and remain to be resolved. Several criticisms ranging from the economic[35] to the feminist[36] have been made. The starting point to much of this criticism is the premise that legitimate "countervalues" to privacy do exist.[37] A sampling of the primary charges and of the grounds for defense follow:

Firstly and fundamentally, a lack of uniform and independent content is presumed by critics of the privacy right. The contention is that the search for a means to codify and give effect to privacy rights is an unnecessary one, since it does not contain any interests which are not already subsumed within the rights to protection of person and of property. The attack is two-fold: there is reference to a lack of specificity of content and to a lack of independent

---

33 Finnis, *supra* note 30, 210.

34 *Id.,* 198.

35 *See* Posner, *infra* note 50.

36 *See, e.g.,* Catherine A. MacKinnon, Toward a Feminist Theory of the State (1989) (MacKinnon argues that protection of the private space could result in the invisibilization of abuse and perpetuate a system of silence contrary to women's interests); Reva B. Siegel, *"The Rule of Love": Wife Beating as Prerogative and Privacy*, 105 Yale L. J. 2117 (1996); Ruth Gavison, *Feminism & The Public Private Distinction*, 45 Stan. L. Rev, 21 (1992); Anita L. Allen & Erin Mack, *How Privacy Got Its Gender*, 10 N. Ill. U. L. Rev. 441 (1990) (in which the authors critique the seminal Warren and Brandeis formulation of privacy through a feminist lens).

37 *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1217 (1998) (Professor Kang argues that, in general, the provision of privacy rights will have to balance the "countervalues" to privacy as well.).

content. As to the first, critics contend that the lack of specificity and uniformity of the right's content stem from the confusion in its definition. As discussed hereinbefore,[38] we reply that, in the first place, much of this fog can be lifted by adopting a pragmatic and reductionist account of the term- where privacy is consistently construed narrowly, to eliminate (or minimise) overlap with other concerns such that the core concerns against which privacy serves to protect individuals are covered. At any rate, a charge of vagueness of the term should not detract from a recognition of its value as a right or interest which merits protection in legislation as well as in adjudication. It is also useful to distinguish between the *right* and the *concept*,[39] with the former referring to what we can accept must involve legal protection and the latter to what we recognize as being private in more general and less technical terms. On such an understanding, it is clear that a workable law need not concern itself with what privacy is and must only determine what circumstances of privacy require protection.[40] Further, and at the cost of repetition, lack of consensus on how to operationalise the right should not pre-empt the conclusion that the right itself is a valuable one. It is particularly noteworthy that several important and practically relevant principles of common law seem *prima facie* vague by reason of the lack of an apparent or precise definition. It has been argued that the infringement of privacy can, in that sense, be likened, for instance, to the law relating to negligence in private law or to *Wednesbury* unreasonableness at public law.[41] The argument advanced in defense of legislating for privacy is essentially that even as procedural wrinkles arise to be grappled with, the principles (of privacy being understood as a non-absolute right which must be protected against countervailing State or societal interests), are basically sound and amenable to application as legal concepts in lawmaking and in adjudication.[42]

Secondly, it has been asserted that cultural relativism will imply that there is no socio-cultural impetus acknowledging the public-private dichotomy and the need for protection against private harms. In the specific context of India, the prevalence of a "culture of trust", in contrast to one of privacy, is cited as an historic and social fact militating against the positive provision of privacy rights.[43] The fact that all liberal democraries recognize the need for and the value of protecting individual rights and liberties, the fact that there is a wide field in India as elsewhere for privacy harms to arise and the proliferation of intrusive technologies which create a new and growing risk of privacy harms all militate against such an argument. Contending that no right of privacy should be recognized in India because social mores or institutions

---

38 *See supra* Part-II.

39 Daniel J. Solove & Paul M. Schwartz, Privacy And The Media 39 (2008).

40 Hyman Gross, *The Concept of Privacy*, N.Y.U. L. Rev. 34, 36 (1967).

41 Alec Samuels, *Privacy: Statutorily Definable?*, 17 Statute L. Rev. 115, 118 (1996).

42 *Id*.

43 Subhajit Basu, *Policy-Making, Technology & Privacy in India*, 6 Indian Journal of Law And Technology 65 (2010). *See also* Bhikhu Parekh, *Private and Public Spheres in India*, 12 Critical Rev. Int'l Soc. & Pol. Phil. 313, 317 (2009).

will differ as between societies, and that the prevelant ethical obligations will also vary in consequence, is fallacious. Indeed, it is recognized that such variances and cultural relativities in general are inconclusive of whether ethics of those societies will vary as a consequence.[44] Finnis, for instance, demonstrates that the alleged problems of reductionism, cross-categorization and the extent of variety of lists of the basic and 'universal' human values can be overcome even where they do exist.[45]

Notwithstanding the defense against privacy as culturally relative and consequently, alien to India on *historical* facts, it should not disallow institutional protection of privacy if a *present* need for it can be shown to have arisen. The new concerns brought up by emergent technologies butress the argument for protection against privacy harms considerably. New media and technologies have given rise to an unforeseen panoply of new risks to privacy interests. Among them are the increasing amount of data flowing to and being held by intermediaries providing data on the internet, which the data subject never intended to reveal, for instance. Indeed, Posner recognises that "one cannot negotiate modernity without continuously revealing personal information", resulting in a "radically diminished informational privacy" and a "new culture of transparency" in the electronic age.[46] Significantly, technological advances have meant that there is diminishing control of persons, both natural and legal, over their identity and other information, and an increasing subjects' vulnerability resulting from the heightened risk of unchecked exploitation.[47] Even if we were to assume that existing approaches to privacy protection constituted complete accounts, the pressures of technology have rendered them inchoate.[48] A logical response to these changes would be to ensure privacy protection which is able to preserve privacy in general and continuously relevant terms in the face of more and changing privacy-invasive technologies. Recent legislation in the country has, however, failed to achieve this.[49]

---

44 *See* Carl Wellman, *The Ethical Implications of Cultural Relativity*, 60 Journal of Philosophy 169 (1963).

45 Finnis, *supra* note 30, 82.

46 Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245 (2008). *See also* George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. Legal Stud. 623 (1980); James S. Coleman, *An Introduction to Privacy in Economics and Politics*: *A Comment*, 9 J. Legal Stud. 645 (1980).

47 David W. Leslie & Alton L. Taylor, *The Issue of Privacy Reviewed*, 1 Research in Higher Education 119, 120 (1973) ("A primary threat to individual and institutional privacy lies with the collection, interpretation, or dissemination of information which is beyond that individual's or institution's control.").

48 *See, e.g.,* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. On Telecomm. & High Tech. L. 357 (2010-11) (Richards makes this assertion in the context of the prevalent fourfold tort system in the US).

49 *See, e.g.,* Apar Gupta, *Balancing Online Privacy in India*, 6 The Indian Journal of Law and Technology 43 (2010) (Gupta reviews the state of the Information Technology Act, 2000 after the passage of Information Technology (Amendment) Act, 2008, and its insertion of § 69 in particular to conclude that procedures for online surveillance in India do not do enough to safeguard inviduals'privacy for several reasons, notably the absence injury discovery and

Another significant argument is that comprehensive protection of private spaces through a system of privacy rights detracts from the full achievement of economic efficiency in the marketplace.[50] Operating on an understanding of privacy in the limited sense of the concealment of information, Posner's influential critique of normative accounts of privacy as having a deterimental impact on the market for information led him to conclude that much of the concealment of personal information allowed in societies was misguided.[51] Specifically, it is his case that privacy, understood as concelament of information, could impede economically efficient resource allocation by reducing the amount of information available in the marketplace. While this is a concern, it must be recognized that regulation is not necessarily or always geared towards economic ends. Governments also regulate toward social ends, with the intent that rights seen as non-negotiable are secured. A Kantian view of the issue would clearly reveal the need for protection of some interests for being ends in themselves.[52]

In addition to the above defences, it is also possible for privacy rights advocates to contend that a failure to protect privacy will have adverse consequences for the protection of rights that are already guaranteed to citizens. In jurisdictions lacking a general privacy protection, citizens are compelled to turn to seclusion and self-censorship in order to defend private and intimate spaces, thus creating societies of "reasonable paranoids".[53] Elizabeth Paton-Simpson uses the term "reasonable paranoids" to add a new dimension to what is already understood as the chilling effect. She argues not only that self-censorship will be a consequence of a loss of privacy (this is the chilling effect on speech and conduct) in the absence of laws protecting it, but also that where courts consider privacy questions, applying the device of a reasonable person does nothing to actually deliver the right. This is because the fiction of the reasonable person correpsonds, in her argument, to a person who is in fact more cautious than the ordinary, rational person in practice. Arguably then, the failure of a grant of *effective* and clearly articulated privacy protection to citizens has consequences for other non-negotiable rights. The rights to freedom, especially of speech, of conscience and to assembly, association, movement and other expressive conduct, all become subject to infringement.

---

redressal mechanisms within the law's 'privacy-by-procedure' framework and the failure to account for the fundamental variance of the character and harms arising out of online surveillance when comapared to telephone tapping.).

50 Richard A. Posner, *The Economics of Privacy*, 71(2) American Economic Review 405 (1981); Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393 (1978); Richard A. Posner, Overcoming Law 531-551 (1995). But Posner's critique has not gone unanswered. *See, e.g.,* Edward J. Bloustein, *Privacy is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 Ga. L. Rev. 429 (1978); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L.J. 2381 (1996).

51 Posner, *The Economics of Privacy*, *id*, 406, 408.

52 *See supra* Part-III.

53 Elizabeth Paton-Simpson, *Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places*, 50 University of Toronto L. J. 305, 307 (2000).

V. HOW THE RIGHT COULD BE OPERATIONALISED: SOME PRELIMINARY CONCERNS

Arguably, privacy, as with any right or interest, can be protected in any of several ways. The three primary means available are, first, by a *lais-sez-faire* approach encouraging and allowing self-regulation;[54] second, through privacy-enabling technological architecture, particularly where communication media such as the Internet are involved; and finally, through state action, whether through a general and all-purpose law or through piecemeal, sectoral laws.

Self-regulation is generally understood as the governance of a given market by its participant actors themselves, without State contribution or coercion. The argument flows that the marketplace will define (and may operationalise) privacy rights in the absence of a legislative prescription under such a regime. But the risk that arises with self-regulation is that this will only be to the degree that information collectors, whether of governmental or commercial affiliation, choose to do so, and no further, even in the face of a moral justification for a more expansive right. In essence, the problem with such an approach is that the marketplace, and particularly its supply-side, will not value non-economic considerations the preference for which consumers are unlikely to convey and assert in any material terms.[55] It is useful to characterise the problem as one involving an imbalance of power, where individual consumers as data subjects, as with price takers in the economics of competition, will have to take the privacy default that information collectors and processors will offer in exchange for their services as given rather than as being subject to determination by the push and pull of market forces.

Second, incorporating privacy-enhancing technology into spaces requiring privacy protections is a valuable tool to preserving private lives and spaces. As a matter of acheiving the realistic protection of the right, pro-active measures such as these, which would build architecture to preserve privacy as the default, rather than measures to expunge unwanted publicity to private facts after the fact, are clearly more pragmatic. Privacy as the default setting in online communications, for instance, could have gone a long way in preventing the loss of privacy which measures such as the EU's recent proposal for a

[54] There exists, of course, the potential for a mixed mechanism of co-regulation, for instance, to be adopted.

[55] Mike Feintuck, *Regulatory Rationales Beyond the Economic: In Search of the Public Interest* in The Oxford Handbook of Regulation (2010) 39-60 (Feintuck makes the argument herein that public interest objectives will have to be delivered otherwise than by purely market-driven regulation).

right to data erasure[56] seek to correct. On the other hand, systems such as Ann Cavoukian's principles for "privacy-by-design"[57] have been influential in recognizing the need to create privacy preserving technologies and in articulating the specifics of what such systems should be able to acheive. We would aver that this is an important means by which privacy can and should be protected. The impetus for such changes to be made will, however, lie on the market, whose failures we have just outlined above, or on an expert or specialist standards regulator who sets and oversees the implementation of the requisite standards, such as the FTC in the United States.[58] This would be the case because laws must, of nature, be technologically neutral in as much as they should be able to exist and have relavance independent of the often short lifecycles of techonolgies, from their introduction to their ultimate obsoloscence.

Even where the State does legislate to protect privacy rights, piecemeal and sectoral laws are subject to the criticism that ostensible rightholders are unable to locate their rights or assert them in general terms. In fact, in the context of Prosser's privacy torts,[59] such an approach has been criticised as being fragmentary.[60] Also, information gathering, storage and processing is now a fact of modernity, and laws governing privacy should aim at achieving a fair balance of the interests implicated (those of the state and public authorities *vis-à-vis* those of the data subject) given that there is tangible room for a situation of competing interests to arise.[61] These will likely cut across legislative fields in their subject-matter and require some degree of harmonisation. A single, unifying legislation is best able to achieve this.

While the reductionist approach[62] will lead to certainty as to content in interpretation and adjudication, the impetus placed on advancing normative ends, over and above those that exist and can already be described in the right to privacy discourse, must be accounted for. The civil law instrument of 'optimal generality'[63] may prove a useful guide in situations such as the one

---

[56] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final, Art. 17.

[57] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, available at www.ipc.on.ca/images/resources/7foundationalprinciples.pdf (Last visited March 29, 2012).

[58] *See, e.g.,* Hayley Tsukayama, *FTC privacy: Key exerpts from the report*, March 27, 2012 available at http://www.washingtonpost.com/business/technology/ftc-privacy-key-excerpts-from-the-report/2012/03/26/gIQAYXjUcS_story.html (Last visited on March 30, 2012), Ryan Singel, *FTC Tells Net: Stop Invading Privacy (Or We'll Say 'Stop' Again)* available at http://www.wired.com/threatlevel/2012/03/ftc-privacy-report/ (Last visited on March 30, 2012).

[59] *See infra*, Part-VI.A.2 (Prosser's torts break privacy harms down into four distinct categories.).

[60] *See* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962 (1964).

[61] *See, e.g.,* Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 74 U. Chi. L. Rev. 343 (2008).

[62] *See supra*, Part-II.

[63] René David & John E. C. Brierley, Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law 94-98 (1985).

at hand. An effective law in such a case would be one which has achieved the right degree of abstraction, such that laws are conceptual in nature, allowing for both longevity and a breadth of application. Indeed, the model of an omnibus privacy law to which laws governing specific sectors are anchored has proven workable in Germany[64] and later in the EU[65] in the context of informational privacy.

Thus, crystallising a general right would have, we argue, the best result. The action will clearly reflect on the legislative concern for individual's privacy and the proetction that it deserves in light the foregoing dicussion.

VI. TWO PARADIGMS OF PRIVACY RIGHTS

A. THE RIGHT TO PRIVACY IN THE UNITED STATES: SALIENT FEATURES

The United States' privacy protections span its Constitution, sectoral state and federal statutes and a scheme of remedies in torts. Of these, the first and last are of significance, having historically, theoretically and practically shaped the landscape for privacy protections in the US.

1. The Constitutional Discourse[66]

Early judicial pronouncements as to the right's constitutional status were visibly moral in their construction, as with the US Supreme Court's first statement on the point: "the right to be let alone- the most comprehensive of rights and the right most valued by men".[67] It is of some interest to the questions at hand to note that the US Constitution, like the Indian Constitution, provides for no explicit constitutional right of the individual to his privacy. Much of the canon establishing that the right exists and is accorded constitutional status is consequently grounded in articulations of the right in the adjudicatory sphere. Many of the landmark privacy cases have involved questions relating to reproductive and sexual autonomy, but this is not to suggest that the constitutional right has not otherwise been relevant.[68] Indeed, it has been emphasised

---

64 Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) ('Federal Data Protection Act'), January 27, 1977, BGBl.

65 Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data ('EU Data Protection Directive').

66 *See generally* Lawrence H. Tribe, American Constitutional Law, Vol. II, 1302-1435 (1988).

67 Olmstead v. United States, 277 U.S. 438 (1928), 478. (Brandeis, J. dissenting).

68 *See, e.g.,* NAACP v. Alabama, 357 U.S. 449 (1958) (This involved associational privacy, and the right to privacy in the membership list of an association under the First Amendment in particular); Katz v. Unites States, 389 U.S. 347 (1967) (The US Supreme Court articulated the "reasonable expectations of privacy standard" in relation to the interception of communications under the Fourth Amendment here); US v. Antoine Jones, Docket No. 10-1259, Decided

that while sexuality was the predominant (though not exclusive) concern in these cases, the doctrine itself is of wider application.

With *Griswold* v. *Connecticut*,[69] through a device of penumbral rights, a broad constitutional privacy right emanating out of basic guarantees in the Bill of Rights (particularly the immunity from unreasonable search and seizure, the guarantee against self-incrimination and the general restriction on quartering armed forces personnel in civilian residences, etc.) was explicitly recognised as inhering in the marital relationship, despite its absence in the constitutional text. Later affirmations came most notably in *Eisenstadt* v. *Baird*,[70] clarifying that privacy was an *individual* right, and in the celebrated *Roe* v. *Wade*,[71] in which the scope of the right was held by a majority to extend to a woman's right to choose whether to terminate her pregnancy.

Another particular constitutional space that deserves mention for our present purpose is the treatment of privacy considerations with regard to search and seizure by the State under the Fourth Amendment. Questions that arise under this category impute privacy concerns, along with the limits on the State's power to surveil. *Katz* v. *United States*[72] marks a turning point for the way in which privacy is viewed in law. Justice Harlan's concurrence brought some clarity to the law on the point by his seminal finding that the Fourth Amendment would disallow searches where the suspect had what he termed a "reasonable expectation of privacy", *i.e.*, a subjective and personal expectation of privacy as well as a societal recognition of that expectation as a reasonable one.

Later case law has continued to apply this standard as a touchstone,[73] although the emergence of a "third-party doctrine", under which a rightsholder's privacy interests stood dissolved once information was shared with another seemed to suggest that privacy as informational control or decisional autonomy with relation to private papers and information did not find protection in this scheme. Also of note is a more recent holding of the US Supreme Court in its first affirmation of the right to geo-location privacy in *Unites States* v. *Antoine Jones*,[74] in which the Court found that the continuous and warrantless use of a tracking device by law enforcement officials on a criminal suspect's motor vehicle constituted a "search" that was violative of

---

January 23, 2012 (This involved an affirmation of the right to geo-location privacy, even where it was visible on public streets).

69 381 U.S. 479, 482-487 (1965).

70 405 U.S. 438, 453 (1972).

71 410 U.S. 113 (1973).

72 389 U.S. 347 (1967).

73 *See, e.g.,* United States v. Miller, 425 US 435, 442 (1976); Smith v. Maryland, 442 US 735 (1979); Oliver v. United States, 466 US 170, 178 (1984); California v. Greenwood, 486 US 335 (1988); Florida v. Riley 488 US 445, 450 (1989).

74 Docket No. 10-1259, Decided on January 23, 2012.

his reasonable expectation of privacy. Justice Sotomayor's concurrence on the grounds that the fact that presents, for the first time since the Court's acceptance of the third-party doctrine, a reasoned case for its inadequacy to address privacy harms.[75]

It is evident from the above that there is a clear, consistent strain in US constitutional thought surrounding privacy rights that sees the right as, to a great degree, limiting State intrusion into private spaces.

2. The 'Right of Privacy' in Torts

The US saw its first notable mention of a privacy right or interest in a seminal paper,[76] in which a distinct 'right to be let alone' was sought to be derived from common law torts. The case for this right was made in the context of an increasingly intrusive press in an attempt to address the inadequacy of existing protections on dissemination of personal information by the press in particular (those being limited to the torts of libel or defamation, in which the defense of truth was available by definition).[77]

In 1960, Prosser posited a groundbreaking formulation of a four-fold system of privacy torts emphasing the nature of the conduct and injury in each case.[78] The formulation has been hailed for bringing together doctrinaire (and academic) considerations and the demands of practice.[79] Prosser's formulation identified four types of privacy-invasive activity for which redress could be sought based on a comprehensive analysis of precedent. These were: (1) unreasonable intrusion into the individual's seclusion, (2) appropriation of name or likeness, (3) bringing unreasonable publicity to the individual's personal life, and (4) publicity in false light.[80]

These, however, are not exhaustive. Prosser's formulation is unable, for instance, to "accomodate the privacy interests implicated by networked technologies".[81] Danielle Citron argues that this is the case because Prosser built his system of torts on precedent and a limited and specific list of privacy harms which is too narrow to respond to the new and changing list of interferences with privacy that we are faced with at present. More problematically, the formulation has proved susceptible to a "writ system" approach, by which the

---

75 *Id*.

76 *See* Warren & Brandies, *supra* note 12.

77 Neil M. Richards, *The Puzzle of Brandeis, Privacy & Speech*, 63 Vand. L. Rev. 1295, 1302 (2010) (Richards contends that the point of the exercise for Warren and Brandeis was to insulate social elites from an increasingly intrusive penny press marketed to their social inferiors).

78 William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960). S*ee also* Restatement (Second) of Torts (1997).

79 Danielle Keats Citron, *Mainstreaming Privacy Torts*, 99 Cal. L. Rev. 1805, 1831-1850 (2011).

80 *See* Prosser, *supra*, note 78.

81 *See* Citron, *supra* note 79, 1806, 1831-1850.

list of torts is treated as exhaustive and no remedy can be granted unless harm under one of the four enumerated heads is shown.[82]

B. PRIVACY & DIGNITY: THE CONTINENTAL PARADIGM

In juxtaposition to the US construction of the privacy interest and the values that undergird it, civil law traditions in Europe and the EU have located their privacy rights in the discourse surrounding essential human dignity and respect, rather than in classical understandings of liberty. This difference in sensibilities has been attributed to the differing juridified intuitions of socio-cultural values in American and European societies.[83] In general, while the US zealously guards against State intrusions, its liberty paradigm fails to place adequate emphasis on the protection of identity and personal information. The treatment of privacy rightsholders acting in the capacity of consumers in online and real space commerce is symptomatic of this failure, in as much as personal information is exchanged and transacted in freely by commercial interests and remains considerably under-regulated in comparison to interfernces with the same data by the State. On the other hand, while the dignity paradigm is less belligerent to State surveillance, it remains elementally concerned with the protection of person, image, reputation and personal information.[84]

Art. 8 of the European Convention for Human Rights is the source of the privacy rights for EU citizens, granting citizens the right to respect private and family life, the home and correspondence of individuals and casting on Member States the obligation to ensure, by means of legislation, that citizens' privacy rights are protected.

The text of the Article and the European Court of Human Rights' ('ECtHR') jurisprudence[85] on personal autonomy both typify this continental sensibility. The former recognizes that the right to privacy is not absolute and, accordingly, the focus of the Court has been to determine whether the interference with the right is reasonable, in the circumstances. The inquiry proceeds on whether a three prong test is satisfied: the State must demostrate that the interference with privacy is prescribed by law, that it serves what the Court will recognize as "legitimate aims" under the Charter and that it is necessary and amounts to a proportionate interference in the circumtances. The Court has consistently recognized that the exercise of preserving privacy involves, in

---

[82] David W. Leebron, *The Right to Privacy's Place in the Intellectual History of Tort Law*, 41 CASE W. RES. L. REV. 808 (1991).

[83] *See* Whitman, *supra* note 10, 1110.

[84] *Id.*

[85] *See, e.g.,* Caroline Von Hannover v. The Federal Republic of Germany, [2004] ECHR 294; Reklos and Davourlis v. Greece, [2009] ECHR 200.

the main, a balancing of rights such that the right and legitimate countervailing interests do not operate to negate the other.[86]

The latter has rightly recognized that the term "private life" is, of its nature, incapable of exhaustive definition.[87] As a result, the Court's approach is to examine whether there has been an interference with privacy in light of the circumstances of each case. The Court has found that the collection of information by State officials without obtaining consent, whether it is demographic information collected for the purpose of a census,[88] finger prints or photographs.[89] In the realm of State surveillance, the ECtHR has been a strong advocate of safeguards in procedure such as notice and review. In its seminal holding in *Klass* v. *Federal Republic of Germany*, the Court held that secret surveillance, *i.e.*, surveilling after imposing a requirement of non-notification to the subject will *ipso facto* raise an Art. 8 issue.[90] In other words, the mere existence of a law allowing secret surveillance will amount to an interference with privacy. Further, there has been a consistent affirmation of the fact that surveillance must be undertaken under a statute,[91] rather than be left purely to administrative discretion.[92] The Court seems by this to acknowledge that data subjects must have the right of informational autonomy in relation to data that relates to them. Presciently, the Court has also recognized in explicit terms that privacy is adversely affected where there is data aggregation, *i.e.*, where information is systematically collected and then stored and viewed together.[93] Aside from surveillance, interference by the State with personal identity elements, such as one's name even where a legitimate interest exists has been found to be violative of Art. 8.[94]

The EU has also been zealous in recognizing member-states' obligations to protect against horizontal violations of privacy, with the role of the media finding particular concern.[95]Another area in which the evolution of EU law has been rapid has been in relation to data protection legislation to protect data subjects' autonomy and control over information relating to them. These data protection and privacy directives attempt to specify the duties of intermediaries such as service providers on the internet, mobile service providers

---

86 *See, e.g.,* Gaskin v. The United Kingdom, (1989) 12 EHRR 36, ¶42.
87 Costello-Roberts v. The United Kingdom, Series A, No. 247C (1993), ¶36.
88 X v. The United Kingdom, October 6, 1982, 30 DR 229.
89 Murray v. The United Kingdom, Application no. 14310/88, Judgment of October 28, 1994.
90 Klass v. Germany, Application no. 5029/71, Judgment of September 6, 1978, ¶36.
91 Khan v. The United Kingdom, Judgment of May 12, 2000.
92 Malone v. The United Kingdom, Application no. 8691/79, Judgment of August 2, 1984.
93 Rotaru v. Romania, Application no. 28341/95, Judgment of May 4, 2000.
94 Stjerna v. Finland, Series A no. 299-B.
95 Caroline Von Hannover v. The Federal Republic of Germany, [2004] ECHR 294; Parliamentary Assembly of the Council of Europe, *Resolution 1165 (1998): Right to Privacy* available at http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta98/eres1165.htm (Last visited on March 29, 2012). *But see* Von Hannover v. The Federal Republic of Germany (No.2), Application nos. 40660/08 and 60641/08.

etc. in relation to the treatment of data and to limit the discretion that States have with respect to surveillance by prescribing maximum limits for data retention and emphasising the general need for the data subject's knowledge, if not consent.[96]

Also, a path not adopted in the US but which has found emphasis across the Atlantic in Germany is that of a unitary right of personality, from which more than the four aspects that Prosser posits follow.[97] The breadth of the German formulation allows for particular protections such as an absolute restriction on the violation of "core areas of life", which are unavailable in the US, by virtue of the uniform approach of balancing competing interests.[98]

VII. PRIVACY & THE LAW: A BRIEF SURVEY OF THE INDIAN MILIEU

A. LOCATING THE INDIAN STATE'S OBLIGATIONS TO PROTECT PRIVACY AT INTERNATIONAL LAW

There is clear evidence of a global consensus as to the fact that privacy is a value and a legal interest worth protecting, inasmuch as States have voluntarily chosen to incur legal obligations to protect the privacy interest of their citizens. The Indian position in this regard is explained in the following paragraphs.

India is one of the largest destinations for the outsourcing and processing of personal information in the world and this has led to increased scrutiny of its data protection laws (or indeed the perceived lack thereof). The Universal Declaration of Human Rights[99] ('UDHR'), adopted by the General Assembly of the United Nations in 1948 represented the first comprehensive agreement among nations on the specific rights and freedoms of all human

---

96 *See, e.g.,* Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council of November 25, 2009 Directive 2006/24/ECs Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks; roposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

97 *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CAL. L. REV. 1925 (2010).

98 *Id.*

99 Universal Declaration of Human Rights, December 10, 1948, G.A. Res. 217A (III), U.N. Doc. A/810.

beings. India voted in favour of the UDHR. Art. 12 of the UDHR discusses the right to privacy and states that an individual would have the right to protection of the law against any arbitrary interference.[100] The International Covenant on Civil and Political Rights ('ICCPR'), also adopted by the United Nations General Assembly (in 1966), was signed by India on April 10, 1979. Art. 17 of the ICCPR discusses the right to privacy in terms similar to the European Convention, *i.e*, as a right against arbitrary interferences with privacy, with that arbitrariness being determined by the three prong test.[101] India has not, however, signed Optional Protocol-I to the ICCPR, as a result of which it is not possible for Indian citizens to make a complaint concerning failures to fully implement Art. 17.[102]

Indian courts have been influenced by customary international law despite the failure of the legislature to sanction it. The Supreme Court has endorsed the doctrine of incorporation by which customary international law has an immediate effect on domestic law.[103] In *Gramophone Co. of India Ltd.* v. *Birendra Bahadur Pandey*,[104] it stated that rules of international law may be incorporated into domestic law even without sanction by the legislature, provided they did not conflict with Acts of Parliament.[105]

B. LOCATING PRIVACY PROTECTIONS IN LEGISLATION EXTANT

Although the National Commission to Review the Working of the Constitution recommended that an Art. 21-B (granting a constitutional right to privacy) be inserted into the Constitution by amendment,[106] that

---

[100] *Id.* (Art. 12 provides: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence...").

[101] UN Human Rights Committee, *General Comment 16* in 'Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies' (1988) UN Doc HRI/GEN/1/Rev 6.

[102] Graham Greenleaf, *Promises and Illusions of Data Protection in Indian Law*, 1(1) International Data Privacy Law (2011).

[103] Michael P. van Alstine, *The Role of Domestic Courts in Treaty Enforcement: Summary and Conclusions*, in The Role of Domestic Courts in Treaty Enforcement: A Comparative Study (2009).

[104] (1984) 2 SCC 534: AIR 1984 SC 667.

[105] *Id.*

[106] National Commission to Review the Working of the Constitution, A Consultation Paper on Enlargement Of Fundamental Rights, May 11, 2001. (The recommended article text reads: "(1) Every person has a right to respect for his private and family life, his home and correspondence (2) Nothing in Clause (1) shall prevent the State from making any law imposing reasonable restrictions on the exercise of the right conferred in clause (1), in the interests of the security of the State, public safety or for the prevention of disorder or crime, or for the protection of health or morals, or for the protection of the rights and freedom of others." This formulation is consistent with that of international rights instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention on Human Rights, *inter alia*).

recommendation never came to fruition. Also, India lacks effective and inclusive privacy coverage in legislation, although there are some scattered attempts to address it in specific contexts, such as in the IT law, the Right to Information Act and consumer protection laws, etc.[107]

Concerns over the legislative treatment of sensitive information in cyberspace[108] have now emerged as a predominant concern. At present, although there is no law even dealing specifically with data protection in India, there are various existing laws that provide safeguards in the fields of banking, contractual relations, telecommunications, etc. The Telecom Regulatory Authority of India, which regulates telecommunications in India, released a Common Charter of Telecom Services in 2005 in accordance with which service providers must ensure that the privacy of their subscribers is protected, subject to State interests such as national security.[109] The Telegraph Act, 1885[110] permits audio surveillance *via* telephone tapping, subject to procedural directions laid down by the Supreme Court in the interests of privacy rights of citizens.[111] Elsewhere, the Credit Information Companies (Regulation) Act, 2005 requires participants in credit reporting to adopt principles covering every aspect of data protection.[112]

Importantly, there is also the Information Technology Act, 2000 ('IT Act'), which provides recognition to and regulates electronic commerce, and deals with computer and cyber crimes, hacking, damage to computer source code, breach of confidentiality and viewing of pornography. The particular legislative attention paid to cyber-security is evident in the grant of powers under this Act to governmental authorities and agencies to facilitate their investigation of cyber crimes. §69 in particular gives the Controller of Certifying Authorities the power to direct a government agency to intercept information transferred through computer resources if the Controller is satisfied of its expediency to do so in the interest of national sovereignty and security, friendly relations with other States, public order or for preventing incitement to the commission of cognizable offences.[113] Non-compliance with such requests for the disclosure of information will result in monetary liability, in the form of heavy fines.[114]

---

[107] For a comprehensive account of privacy coverage across sectors, *see* The Center for Internet and Society, *Privacy in India-An Early Draft* available at http://cis-india.org/internet-governance/country-report (Last visited on March 29, 2011).

[108] V. Venkatesan, *Cyber Fears*, available at http://www.frontlineonnet.com/fl2813/stories/20110701281304700.htm (Last visited on September 13, 2011).

[109] The Common Charter of Telecom Services, 2005, available at http://www.trai.gov.in/citizencharter/comm_charter16mar2006.pdf (Last visited on September 13, 2011).

[110] The Telegraph Act, 1885, §5(2).

[111] *See* R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471: AIR 1973 SC 157; People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301: AIR 1997 SC 568.

[112] *See* Centre for Internet Society, *supra*, note 107.

[113] The Information Technology Act, 2000, §69.

[114] *Id.*, §44.

The IT Act has been criticized for its treatment of internet intermediaries. The Information Technology (Amendment) Act, 2008 defines an intermediary as a person who, on behalf of another, receives, stores or transmits a record or provides a service with respect to that record.[115] Telecom service providers, network service providers, internet service providers, webhosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafés are included in this definition of intermediary.[116] The IT (Amendment) Act, 2008 was passed to incorporate the recommendations of an Expert Committee set up by the government,[117] including the implementation of reasonable security practices and procedures regarding the handling of sensitive personal data or information, the gradation of severity of and punishment for computer-related offences committed dishonestly or fraudulently. The Expert Committee also recommended amendments to the Indian Penal Code to cover online obscenity, child pornography and video voyeurism.[118]

India's need for a law to protect the personal information of individuals from being misused by third parties, and by companies in particular, is acute. In response, the Personal Data Protection Bill, 2006[119] was introduced in the Rajya Sabha on December 8, 2006 and is expected to proceed within the general framework of the European Union's Directive on Data Privacy, 1996.[120] It provides for the protection of personal data by requiring the data subject's prior consent in relation to the disclosure of any personal information, except where such disclosure is in public interest.[121] Significantly, the Bill applies to both governmental and private enterprises.[122] Also, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which were adopted on April 11, 2011 under the IT Act make some inroads into shielding data subjects from violations of their rights to informational privacy. These Rules are similar to European Union data protection law and impose a number of obligations on companies in an effort to improve the general standard of data protection laws in the country.[123]

---

115 *Id.*, §2(1)(w).

116 *Id.*

117 Department of Information Technology, Report of the Expert Committee on Amendments to IT Act 2000, available at http://www.mit.gov.in/content/report-expert-committee-amendments-it-act-2000-3 (Last visited on September 13, 2011).

118 *Id.*

119 The Personal Data Protection Bill, 2006, available at http://164.100.24.219/BillsTexts/RSBillTexts/asintroduced/XCI_2006.pdf (Last visited on September 13, 2011).

120 Apar Gupta, *The Personal Data Protection Bill, 2006,* September 18, 2007, available at http://www.iltb.net/2007/09/the-personal-data-protection-bill-2006/ (Last visited on September 13, 2011).

121 The Personal Data Protection Bill, 2006, §3.

122 X v. The United Kingdom, October 6, 1982, 30 DR 229.

123 Hunton and Williams LLP, *India Drafts New Privacy Regulations*, May 18, 2011, available at http://www.huntonprivacyblog.com/2011/05/articles/international/india-drafts-new-privacy-regulations/ (Last visited on September 13, 2011).

They place restrictions on data collection and processing, international data transfers and third party disclosures, and mandate that prior consent of the data subject be obtained before sensitive personal data relating to him or her is processed.

C. JUDICIAL ARTICULATIONS OF A CONSTITUTIONAL PRIVACY RIGHT

The Constitution of India makes no textual or explicit grant of a discretely enumerated privacy right. The Supreme Court has, however, in a number of decisions, interpreted the right to life and personal liberty guaranteed under Art. 21 to include the right to privacy (and has made some indication of a privacy tort, as well). An overview of the judicial pronouncements in the field will show that since the Supreme Court has refrained from defining privacy, the validity of a claim involving a right to privacy will become subject to the facts of the case and to the view taken by the Court in light of those facts.[124]

Although the Supreme Court entertained a substantial right to privacy question in *M.P. Sharma* v. *Satish Chandra*[125] as early as in 1958, *Kharak Singh* v. *State of Uttar Pradesh*[126] was the first influential articulation of the right. Subba Rao, J. stated for the minority that the right to personal liberty not only referred to freedom from restrictions on one's movements but also to freedom from encroachments on one's private life.[127] This view was carried forward in *Gobind* v. *State of Madhya Pradesh*,[128] where the Court held that the right to privacy could be derived from Arts. 19(1)(a), 19(1)(d) and 21, and that it was thus subject to reasonable restrictions. The aforementioned cases primarily discussed the right to privacy with regard to the police and the State's powers of surveillance.

With the decision in *R. Rajagopal* v. *State of Tamil Nadu*,[129] the Supreme Court was able to address another facet of the right to privacy. It held in a question involving the press that details of an individual's life could be published without his consent or authorization only insofar as they appear in public records.[130] Notably, the Court recognized that invasion of privacy claims under Indian law can be of two classes: constitutional challenges based in the right to life and tortious claims for intrusion into privacy.[131]

---

[124] M.P. Jain, Indian Constitutional Law, Vol-1, 1624 (Ruma Pal & Samaraditya Pal eds., 2010).
[125] AIR 1954 SC 300.
[126] AIR 1963 SC 1295.
[127] *Id.*
[128] (1975) 2 SCC 148: AIR 1975 SC 1378.
[129] (1994) 6 SCC 632: AIR 1995 SC 264.
[130] *Id.*
[131] *Id.*

Another context in which the right was affirmed involved surveillance by means of telephone tapping. In *R.M. Malkani* v. *State of Maharashtra*,[132] the Supreme Court stated that the telephonic conversations of an innocent person would be protected against interference by tapping by the police. The issue was considered again in *People's Union for Civil Liberties* v. *Union of India*,[133] where the Supreme Court stated that the right to hold a telephone conversation without interference can be claimed as part of the right to privacy. §5(2) of the Telegraph Act, 1885 which provides for telephone tapping was held to be constitutionally valid, provided that a competent authority is empowered to pass an order of interception after recording that it is necessary to do so in the interest of the sovereignty and integrity of India, the security of the State, relations with foreign States, public order or to prevent incitement to the commission of an offence. The Supreme Court also laid down procedural directions for exercise of power under the section. Thus, the power of telephone tapping is regulated both procedurally and substantively so as to prevent infringement of the right to privacy of an individual. In 2011, the Court considered the question of telecom service providers' liability to subscribers upon responding to orders for interception of communication in *Amar Singh* v. *Union of India*.[134] The Court found here that the intermediary was liable to verify that the order demanding that interception must be verified to be genuine and to act in the interests of its subscribers' privacy, even as it acted in fulfillment of its duty to assist law enforcement when called on to do so.

The recent, much publicised, incident of interception of telephonic conversations between a corporate lobbyist and a number of prominent individuals including a cabinet minister, leading journalists and corporate figures deserves a mention. Between 2008 and 2009, income tax officials intercepted a number of these conversations with the approval of the Ministry of Home Affairs,[135] which were subsequently leaked to the media. In response to these leaked conversations, a petition was filed in the Supreme Court claiming a violation of the right to privacy of the participants in the conversations.[136] It has been argued that these conversations were all professional conversations and would be available to every citizen as they qualify as information relating to public activity and interest under §8(1)(j) of the Right to Information Act, 2005.[137]

---

[132] (1973) 1 SCC 471: AIR 1973 SC 157.

[133] (1997) 1 SCC 301: AIR 1997 SC 568.

[134] (2011) 7 SCC 69.

[135] *See* Hickock, *supra* note 3.

[136] Gyanant Singh, *No Relief for Tata in Radia Tape Hearing*, India Today (New Delhi) December 3, 2010 available at http://indiatoday.intoday.in/story/no-relief-for-tata-in-radia-tape-hearing/1/121945.html (Last visited on September 26, 2011).

[137] *See* Money Control, *Interview of Supreme Court advocates Prashant Bhushan and Dushyant Dave*, November 30, 2010, available at http://www.moneycontrol.com/news/management/ratan-tataright-to-privacy-_502063.html (Last visited on September 26, 2011).

The individual's right to privacy also extends to the right of reproductive autonomy. This includes the right to use condoms and the right of a woman to abort. In *B.K. Parthasarathi* v. *State of Andhra Pradesh*[138], the Andhra Pradesh High Court held that the right to make decisions about reproduction was personal to the man or the woman in question, and includes the right to choose not to reproduce. The Supreme Court also recognized the confidential nature of a doctor-patient relationship in *Mr. 'X'* v. *Hospital 'Z'*[139] when it addressed the conflict between an individual's right to privacy and another individual's right to be informed. It held that wherein there is a conflict between the right to privacy as a part of right to life and the right to lead a healthy life which is a fundamental right under Art. 21, 'the right whch would advance the public morality or public interest, would alone be enforced through the process of court'[140]. This principle was reiterated in the Court's finding that where an individual suffers from diseases such as AIDS, another considering marriage too has a right to know about the former's health, and that it is open to the doctor or the laboratory holding the said information to reveal such information to persons related to the latter.[141]

Other spaces in which privacy considerations arise have also been adjudicated upon by the Supreme Court, with a notable instance being in relation privacy in financial papers. In *District Registrar and Collector* v. *Canara Bank*,[142] where seizure by a State official of a bank's books was in question, the Court emphasised that privacy was not an absolute right and that it was context-specific. Importantly, the Court also discussed the United States' third party doctrine to find that it did not find application in our country.

The Supreme Court's approach to privacy has had to be on a case-by-case basis. No overarching principles exist to clarify what the legitimate coutevailing interests to privacy are to be taken into account as does the ECtHR's jurisprudence, although Art. 21 does protect against unreasonable procedures or the abuse of discretion by the State generally. No clear, objective and universal threshold or standard, such as that of reasonable expectations in the US, against which cases can be tested to determine whether privacy was violated exists either, even as the Supreme Court has made clear that it will not subscribe to or import the third party doctrine in the *Canara Bank* case. We contend that legislating toward privacy would allow for the law on the point to evolve in a streamlined and coherent way, such that clear precedents could be articulated and consistently applied in succeeding cases, without the need for *ad hoc* determination of cases, without reference to any governing principles.

---

138 AIR 2000 AP 156.
139 (1998) 8 SCC 296.
140 *Id.*
141 Mr.'X' v. Hospital 'Z', (2003) 1 SCC 500.
142 (2005) 1 SCC 496: AIR 2005 SC 186.

VIII. THE DRAFT PRIVACY BILL: EXPECTATIONS OF THE LAW

This section will summarily address the salient provisions of the third working draft of the Privacy Bill, 2011 ('the Bill'), as it stands on date. It needs to be clarified that no official version of the Bill has been circulated and no consultations have yet been announced. The print media announced that the Law Ministry intended to table the Bill as early as the monsoon session of 2011.[143] This section omits references to particular section numbers and undertakes an analysis of the key substantive provisions of the proposed Bill.[144]

The Bill provides for a statutory right to privacy for Indian citizens and endeavours to protect this right by regulating the use and collection of personal information. The statutory right to privacy is made subject to laws in force at the time or orders of courts, and will includes confidentiality of communication, private life, financial transactions, medical and legal information, protection from identity theft and use of photographs, fingerprints, DNA samples and privacy from surveillance.

The Bill defines 'interception of communication' as being inclusive of stopping or intercepting any communication and detention of any such communication. It sets out a large number of procedural safeguards to regulate the interception of communications under §5(2) of The Telegraph Act, 1885. Surveillance, whether by electronic or other means that would reveal private or personal information or adversely affect the individual's right to privacy is prohibited by the Bill. The government can, however, undertake surveillance of a person upon the occurrence of any public emergency, in the interest of public safety or for the purpose of preventing crime or disorder. This prohibition would undoubtedly apply to any sting operation that might be undertaken by the media.

There are also provisions prohibiting the revelation of citizens' personal information in the form of photographs, fingerprints and DNA samples of health information, by other persons or by a government officer in public so as to adversely affect the citizen's right to privacy, which amount to a civil wrong. Personal data can be collected only with the consent of the data subject in accordance with the provisions of laws in force. The Bill also allows the data subject to restrict data processing for the purposes of 'unsolicited commercial communications'.

---

[143] *See* J. Venkatesan, *Bill on 'Right to Privacy' in Monsoon Session: Moily,* The Hindu (New Delhi) June 7, 2011; Abantika Ghosh, *Right to Privacy May Become Fundamental Right,* The Times of India (New Delhi) June 4, 2011.

[144] A copy of the the version of the Bill we review here is available at http://lawandotherthings.blogspot.com/p/primary-sources.html (Last visited September 10, 2011).

Notably, the Bill provides for the establishment of a Data Protection Authority of India which will enforce compliance of all its provisions relating to data, monitor developments in technology to ensure that there is no adverse effect on the protection of data, evaluate laws that are in force at the time and recommend appropriate measures to ensure that they conform with the requirements of this Bill. In addition, the proposed Authority will conduct audits of personal data controlled by a data controller, establish and maintain the National Data Control Registry, investigate complaints of data security breach, issue appropriate orders and report to the government on the desirability of Indian acceptance of international instruments dealing with data protection.

There is also a provision for the setting up of the National Data Control Registry which would be an online database to facilitate the efficient and effective entry of particulars by data controllers. Data controllers would be required to make an entry documenting the purpose for which the data is being processed and the Register would be available for inspection by members of the public. The Cyber Regulations Appellate Tribunal, which was established under the Information Technology Act, 2000,[145] is tasked with adjudicating disputes between individuals and the data controller and entertain appeals arising from orders of the Authority. According to this Bill, individuals who suffer as a result of a contravention of obligations imposed on the data controller will be entitled to compensation to the full extent of the damage suffered. Those adversely affected may also exercise their right to initiate criminal proceedings or bring a civil action against any person acting in contravention of any provisions of the Bill or failing to maintain an accurate record of the individual to his detriment.

IX. CONCLUSION

As concerns about intrusive modernities deepen in line with increasingly technologically-driven social and political relations,[146] the case for the preservation of dignity, autonomy and informational control through the vehicle of enforceable privacy laws gains new and particularly emphatic immediacy.

The fact that this legislative attempt has been undertaken in India means that there is much-needed acceptance of the broad case made above for an explicit statutory statement of the right to privacy. In particular, the Bill makes some progress towards the provision of a statutory privacy right in its

[145] The Information Technology Act, 2000, §48.

[146] Lawrence Lessig, *The Architecture of Privacy*, 1 Vand. J. Ent. L. & Prac. 60 (1999) (Lessig argues that new technologies increase the opportunity for, as well as the fact of monitoring by virtue of the architecture of virtual spaces, *vis à vis* real spaces. Data collection and monitoring are now the norm, rather than the exception.).

attempt at a comprehensive coverage of informational, reputational and bodily privacy concerns. The fact that the definition is expansive in terms of its content and in its coverage of potential violators is a welcome change. With its codification of privacy exceptions in which the State can intrude into private spaces, it constitutes a legitimate attempt to regulate the limits of State intervention. The provisions for civil and criminal remedies for infringment of privacy is also commendable. More specific questions, such as what paradigm of protection this Bill adopts and how far it will be effective to enforce them can only be broached once the law is enacted, on more empirical considerations than the scope of this article permits. For the time being however, we conclude in the result that the legislation would be a welcome step, even though it is no panacea to the problem.