The Four Parts of Privacy in India

BHAIRAV ACHARYA

Privacy enjoys an abundance of meanings. It is claimed in diverse situations every day by everyone against other people, society and the state. Traditionally traced to classical liberalism's public–private divide, there are now several theoretical conceptions of privacy that collaborate and sometimes contend. Indian privacy law is evolving in response to four types of privacy claims: against the press, against state surveillance, for decisional autonomy and in relation to personal information. The Supreme Court has selectively borrowed competing foreign privacy norms, primarily American, to create an unconvincing pastiche of privacy law in India. These developments are undermined by a lack of theoretical clarity and the continuing tension between individual freedoms and communitarian values.

Bhairav Acharya (*bhairav.acharya@gmail.com*) is a constitutional lawyer who is interested in free speech, privacy and technology. He writes at www.notacoda.net

In a celebrated paper in 2006, a leading privacy law expert invoked the despair of God who, like the playwright in Jorge Luis Borges' story "Everything and Nothing," invests the world with a diversity of meanings but lacks one himself (Borges 1985). Privacy, he contends, is similarly amorphous with several connotations but no exact meaning (Solove 2006). Likening the world to a play is not new (Shakespeare 1603), but Borges' playwright was also bemoaning a lack of personal depth when compared to his literary characters. It is true privacy defies definition, but it certainly does not want for depth. There are several theoretical conceptions of privacy, some with rich philosophical and juridical histories. This article will briefly visit a few such conceptions before reviewing four contemporary elements of privacy in India that are influencing the evolution of privacy law.

Privacy in Everyday Life

Privacy expectations are commonplace. This is apparent from the diversity of contexts in which privacy claims are made. Privacy is most easily understood in relation to the body, where the law enforces social norms to protect against unwanted physical contact including assault, but does not criminalise staring. Recent controversies over the wearing of the hijab reveal conflicting expectations of privacy in relation to non-intimate personal features such as the face. In the 2014 case of *S A S* vs *France* (2014), the European Court of Human Rights (ECHR) found the hijab was not protected by the right to privacy to endorse demands for its removal in public places. Privacy is also widely claimed with respect to property. Notions of territorial privacy derive from classical liberalism and the protection traditionally given to homes and family life, which is discussed in more detail later. The castle doctrine—which was summarised by Edward Coke: "An Englishman's home is his castle"—demonstrates the common law's relatively early recognition of the inviolability of the home and the privacy of its residents.

The current global debate on the limits of surveillance deals with communications privacy which, according to some early cases in the United States (US), flowed from the protection given to property. Not all communications are protected. While the old English offence of eavesdropping punished the surreptitious listening of a private conversation in a general setting, current Indian law only protects telephonic, electronic and postal communications from unauthorised interceptions. The privacy of a person's location was recently in issue, when the Indian Penal Code (IPC) 1860 was amended to include the new offence of stalking in Section 354D. But locational privacy is impugned more by telephone and internet service providers as well as police investigation techniques such as cell tower triangulation and even handset-based global positioning system (GPS) tracking.

Data protection is another burgeoning field of law to regulate information privacy. Information that can result in the identification of a person, or "personal data," is strongly protected in Europe and the manner in which it can be collected, processed, stored, used or disclosed is heavily regulated. In contrast, Indian law offers very little protection against commercial or state uses of personal data. While direct marketing through telephones or email has received attention, the manner in which personal data has been commoditised, monetised and non-consensually shared has not. Privacy claims against the state have been raised in relation to the collection of biometric information for the issue of unique identity—"Aadhaar"—numbers.

The Meaning of Privacy

It is important to make a distinction between privacy, intimacy and secrecy since they are often wrongly conflated.

What is intimate is private, but what is private need not be intimate (Gerstein 1978). For instance, the nature of a person's sexual relations is both intimate and private whereas information about that person's credit history may be private but is not intimate. Privacy and secrecy are also confused (Cohen 2010, Neocleous 2002). In everyday usage, secrecy usually conceals wrongdoing that may be, but is not necessarily illegal, such as an illicit extramarital affair (Posner 1979). On the other hand, in certain legal contexts imbued by state interests, secrecy restricts the disclosure of information that may affect the integrity, both real and imagined, of the nation state. Hence, while the intimate life of a minister may, with exceptions, be private, the deliberations of that minister during meetings of the cabinet are secret.

Once synthesised from its semantics and contexts, privacy appears to have three distinct meanings. First, privacy means spatial control. This meaning creates private spaces out of territory; but, while many such privacy expectations are socially negotiated, such as an imagined zone immediately surrounding our bodies, the law only protects these spaces when the territory is privately owned, such as a house (Lessig 2002, Goldring 1984, Litman 2000). Second, privacy means decisional autonomy. This protects personal choices that are intimate, such as a person's reproductive or contraceptive preferences, as well as choices that are played out in public, such as a person's faith or dress sense (Clark 1974). And, third, privacy connotes informational control. While the nature and limits of this control is debated, many laws seek to shield a certain vital amount of personal control over information from others (Westin 1967, Fried 1968).

Beate Rössler likens the meanings of privacy to the layers of an onion (2005). The centre of the onion, the innermost layer, she says, encompasses privacy of the body and other intimate interests. The second layer is compared to the classical liberal understanding of privacy that flows from the traditional public–private divide to protect the family and the home. And the third, outermost, layer of the onion describes economic structures or public civil society in opposition to the state, such as private corporations. This multilayered understanding of privacy appears to survive cultural differences (Zarrow 2012, Pow 2009).

Theoretical Conceptions

The primary conception of privacy flows from the classical liberal construction of the private sphere, based on the understanding that the home, the family, the place of worship, and other intimate spaces and relationships must be shielded from society and the state (McCloskey 1974, McCloskey 1980, De Bruin 2010). The private sphere competes with the public sphere—where private people gather to articulate the needs of society with the state, according to Jürgen Habermas—which invites state activity and regulation (1991). Liberal theorists from John Locke to John Rawls have reiterated the primacy of the family and the home in defining the private sphere and the privacy rights that arise therefrom (Locke 1689, Rawls 1971). But this traditional notion of the public–private divide is patriarchally encoded to presume heteronormative families led by men who solely populate the public sphere, confining women to the home and even shielding domestic violence against women with privacy (MacKinnon 1989, Gavison 1992, Allen 1988). Conceptions of privacy that emanate from the private sphere must survive this foundational critique of liberalism to be persuasive.

In 1890, Samuel Warren and Louis Brandeis built on classical liberal theory to argue a new conception of privacy, which they called the "right to be let alone" (Warren and Brandeis 1890), a phrase borrowed from Thomas Cooley (1888). The expansion of the press in England and the US had led to greater scrutiny of the lives of public figures without an equivalent expansion of legal protection. Warren and Brandeis presented two central arguments. First, they proposed an extension of John Stuart Mill's "harm principle" (1859) to defend against the injury caused by prurient gossip and related invasions of privacy. English common law did not recognise a general tort of privacy, but it did offer the tort of nuisance as well as actions under the laws of defamation and confidence, which they found inadequate. Second, they argued intellectual property law failed to address the mental distress caused by unauthorised publication of personal information. In other words, they critiqued the failure of copyright law to treat the peace of mind of a person as a morally relevant quality, which is what classical liberalism sought to protect in the private sphere.

Warren and Brandeis said the essence of the right to be let alone was not private property but "inviolate personality," but they failed to offer a framework for enforcing this claim. By virtue of the principle of inviolate personality, was information about a person under her control? Yes, according to Alan Westin, who claimed that privacy is the ability of a person to control what information about her should be known to others (1967). This conception of privacy, as control over information, was shared by Charles Fried who pointed out that love, friendship and trust are conditional upon privacy (1968), thereby introducing social utility to the control theory. Julie Inness added nuance by stating that the imperative of control attaches with greater moral force to intimate information rather than impersonal information, bringing the privacy–intimacy distinction into focus once again (1991). However, this conception fails to explain what the control of information should be predicated on. It is a defining characteristic of property that a person who owns it may control it without encumbrance. But, is information about us our property (Moore 1998)?

David M O'Brien disagreed, and criticised the theoretical reduction of privacy to the single value of information control. Instead, he claimed privacy denoted "an existential condition of limited access to an individual's life experiences and engagements" (1979). This conception of privacy in terms of the inaccessibility of a person is improved upon by Ruth Gavison, who says privacy and accessibility are inversely proportional; hence, the greatest degree of privacy is attained when a person is completely inaccessible (1980). But, inaccessibility-based conceptions of privacy must be interrogated to

survive two questions: is the sole inhabitant of an inaccessible place really more private than she is isolated (Schoeman 1984, Solove 2002); and, does a person who is confined to an inaccessible place against her will really enjoy more privacy than she suffers a loss of control (Westin 1967; O'Brien 1979)?

With regard to information privacy, perhaps the most convincing conception is proposed by Helen Nissenbaum who argues that privacy is the expectation that information about a person will be treated appropriately. This theory of "contextual integrity" believes people do not want to control their information or become inaccessible as much as they want their information to be treated in accordance with their expectations (Nissenbaum 2004, 2010, 2011). Since privacy suffers an embarrassment of meanings, its epistemological diversity is an asset, allowing different distillations of the norm to inform dissimilar claims.

Privacy and Press Freedom

An analysis of the debate regarding privacy in India reveals four types of privacy claims. The first claim relates to press freedom. According to Thomas Emerson, while privacy and a free press can coexist mostly in harmony, there are two potential areas of conflict: the first concerns the tort of privacy and the second the right to know (1979). The tort of privacy is an American creation; two of its components clash with the right to publish (Prosser 1960; Emerson 1979). These are cases of (i) embarrassing disclosure of private facts, and (ii) the public casting of a person in false light. Significant attention has been devoted to finding the balance between privacy and press freedom in these cases.

With regard to embarrassing disclosures, some courts have tended to uphold invasive publications when deemed newsworthy, such as a US federal appeals court in *Virgil* vs *Time, Inc* (1975) which contrasts with the English cases of *Campbell* vs *Mirror Group Newspapers* (2004) and *Mosley* vs *News of the World* (2008) and the ECHR decision in *Von Hannover* vs *Germany*. In false light cases, courts have wavered between permitting and disciplining sensationalist but non-defamatory speech such as, for instance, the US Supreme Court judgment in *Time, Inc* vs *Hill*. Despite the Ohio Supreme Court's recognition of the false light tort in *Welling* vs *Weinfeld* 866 N E 2d 1051 (2007), there is a trend of reducing the scope of false light cases for impeding free speech, evidenced by the Florida Supreme Court judgment in *Anderson* vs *Gannett Company* 994 So 2d 1048 (2008).

However, several jurisdictions such as the United Kingdom (UK) and India do not recognise the tort of privacy. English courts have steadfastly refused to declare a tort of privacy, a position confirmed by the House of Lords in *Wainwright* vs *Home Office* (2003). In the absence of a privacy tort to protect against press intrusions, claimants have tried to imaginatively bend other legal principles to their will (Markesinis et al 2004). See for instance, *A* vs *B plc* (2003) and *Douglas* vs *Hello!* (2003) which argued the equitable remedy of confidence, and *Ellis* vs *Chief Constable Essex Police* (2003) which argued administrative law principles governing police powers.

This is not to suggest individuals are at the mercy of a mischievous press; on the contrary, the ease with which defamation claims are made with a view to silence the press, especially investigative journalism, is worrying (Dhavan 2008). Emerson identifies three interesting differences between defamation and privacy: (i) in defamation law truth is a defence, for privacy, truth is the grievance; (ii) defamation seeks to protect reputation, privacy protects peace of mind; and (iii) defamatory attacks on reputation can be publicly ameliorated, whereas public participation aggravates privacy injuries (1979).

In 1961, Lord Mancroft proposed the House of Lords codify a right to privacy to restrain invasive publications. The press could defend itself by proving the claimant was the subject of "reasonable public interest" for any of three reasons; namely, her occupation of a position of authority, her fame as a result of some achievement, or her insertion into the public eye due to a contemporary event[1] (Neill 1962, Pratt 1979). In 1971, the Law Commission of India's 42nd report proposed to make a beginning for privacy law in India by legislating to prevent eavesdropping and unauthorised photography. This formula, adopted by the Indian Penal Code (Amendment) Bill in 1978, proposed a new chapter on privacy. However, it did not examine press freedom and eventually lapsed. In 1981, V N Gadgil of the Congress Party introduced a Right to Privacy Bill in the Lok Sabha, which was fortunately defeated. His motivation appeared to be the prevention of exposes of politicians, an effort he renewed in 1994 (Rahman 1994; Noorani 2011). The 1982 Second Press Commission chaired by Justice K K Mathew rejected Gadgil's bill, endorsed the lapsed proposals of 1978, proposed an extensive categorisation of matters that invited the public interest defence, and ceded the authority to judge improper privacy invasions to the Press Council of India (Government of India 1982).

Privacy and the right to know—often framed as the right to information from public sources—sometimes compete. But this tension is greater than the sum of its parts, for in the 1994 case of *R Rajagopal* vs *State of Tamil Nadu* (1994), the Supreme Court (SC) settled the law on the proposition that only the personal privacy of public officials, consisting of intimate actions and information, is protected. Discord occurs when privacy is claimed in lieu of a breach of confidence remedy which, in my view, is the basic flaw in Ratan Tata's ongoing petition in the Supreme Court in respect of the government's unauthorised disclosure of Niira Radia's intercepted communications and their subsequent publication (*Ratan Tata* vs *Union of India* (2010). However, the "iniquity rule"—described by the maxim "there is no confidence as to the disclosure of iniquity"—would apply to protect the publication of confidential information that reveals culpability.

Privacy from State Surveillance

The second type of Indian privacy claim is in respect of state surveillance, both of property and communications. Liberal societies protect the privacy afforded by private property by requiring agents of the state to obtain warrants prior

to entry. In the early 20th century, American courts went a step further to exclude from evidence anything seized from within private property in the absence of a search warrant (*Weeks* vs *United States*). The "exclusionary rule" strengthens privacy by discouraging illegal searches, and the "fruit of the poisonous tree" principle disqualifies evidence gathered with the assistance of illegally obtained evidence. These principles, which protect privacy rights through rules of criminal procedure and evidence, are at odds with English law, which is solely concerned with the relevance of the material, not its pedigree (*Kuruma, Son of Kaniu* vs *R* (1955). The English position was imported in *R M Malkani* vs *State of Maharashtra* (1973) following which Indian law permits illegally obtained evidence.

In 1928, the Supreme Court of the United States (SCOTUS) was asked in the case of *Olmstead* vs *United States* to extend the exclusionary rule to telephone conversations wiretapped without a warrant. In a close decision, with Justice Brandeis—the co-author of the 1890 article on the right to be let alone—dissenting, the court declined because the cables that carried the telephone conversation were not solely confined to private property. This facile reliance on the notion of private property was overruled in 1967 when people, not property, were declared to be the objects of privacy in *Katz* vs *United States*. In the 1996 case of *People's Union for Civil Liberties* (PUCL) vs *Union of India* (1997), the Indian Supreme Court declared telephone conversations were protected by a construction of privacy that flowed from the right to "personal liberty"—guaranteed by Article 21 of the Constitution, thereby triggering a 1978 judicial test requiring wiretaps to be conducted under a just, fair and reasonable law of Parliament (*Maneka Gandhi* vs *Union of India* (1978)).

However, India's past jurisprudence of surveillance regulation is sketchy. In the 1962 case of *Kharak Singh* vs *State of Uttar Pradesh* (1964), the first surveillance-related constitutional privacy claim was mostly rejected by the Supreme Court when the majority refused to locate privacy in "personal liberty"; however, they did prohibit warrantless entry into the houses of "history-sheeters." Justice Subba Rao famously dissented, finding privacy constituted the essence of "personal liberty" and surveillance had a chilling effect on free expression. In *Gobind* vs *State of Madhya Pradesh* (1975), profiting from the evolution of new American privacy jurisprudence in the intervening years, the court leaned towards, but ultimately held short of, recognising a constitutional right to privacy. The court found if the right to privacy did exist in India, it was subject to the test of "compelling state interest" from which it did not emerge intact.

This scepticism has aided the perpetuation of a relatively stringent communications surveillance regime. The interception provisions of the Telegraph Act 1885 in Section 5(2) and its close cousin the Post Office Act 1898 in Section 26 were enacted to bolster colonial control over a subjugated nation, and were disparaged by P Ananda Charlu and Bishamber Nath who were Indian members of the Imperial Legislative Council.[2] After independence, despite the Law Commission of India's 38th report suggesting in 1968 the reading down of the interception provisions for travelling beyond the pale of constitutionality, the Supreme Court cursorily tested the interception provisions against the right to free speech in the 1996 PUCL case and found they survived. In 2008, similar provisions were included through Sections 69 and 69B of the Information Technology Act 2000 to enable the interception and monitoring of electronic communications. Alarmingly, in the appeal of *State* vs *Navjot Sandhu* (2005) concerning the 2001 attacks on the Indian Parliament, the Supreme Court permitted wiretapped evidence illegally obtained outside the boundaries of these already severe laws, a move likely to embolden the police into greater illegal invasions of privacy.

Privacy as Decisional Autonomy

The third privacy claim is in relation to decisional autonomy, and is founded on the belief that privacy is an essential constituent of liberty, the deprivation of which prevents people from making fundamental choices about themselves. Such a conception of privacy has flourished in the US where the national polity is marked by a greater expectation of individual sovereignty against the impositions of society and the state (Lane 2009). The SCOTUS enforced this account of privacy in two landmark decisions in 1965 and 1973. In the former case of *Griswold* vs *Connecticut*, the court struck down a law that criminalised birth control for violating the inherent privacy of marriage. The majority declared couples had a right to privacy that protected their choices regarding contraception, and this right emanated from the "penumbras" of the other rights in the US Bill of Rights, which together created a "zone of privacy." In the latter case of *Roe* vs *Wade*—more controversial for its subject matter: abortion—the court upheld a woman's decisional autonomy to terminate her pregnancy afforded by the right to privacy, but located this right firmly in the constitutional guarantee of "personal liberty," not amongst the penumbras of other rights.

However, decisional autonomy cases have been inconsistent. In *Bowers* vs *Hardwick* in 1986, the SCOTUS failed to protect private and consensual adult homosexual sex based on an unsound heteronormative application of the classical public–private divide. Dissenting judge Harry Blackmun, who had delivered the primary judgment in *Roe*, condemned the majority's "wilful blindness" to the privacy interests of gay people. In 2003, *Bowers* was overruled by *Lawrence* vs *Texas* which returned the privacy of sexual choice to an expanded interpretation of "personal liberty" in the Bill of Rights. Ironically, while Indian privacy jurisprudence borrows the idiom of personal liberty, it has only applied it with limited success in surveillance-related cases—*Kharak Singh*, *Gobind* and PUCL—where the privacy interests in homes or communications are obvious and bear no relation to decisional autonomy. The sole attempt to enforce decisional autonomy flowing from a right to privacy emanating from the constitutional guarantee of "personal liberty" was made by the Delhi High Court in *Naz Foundation* vs *Government of NCT Delhi* (2009),

but was unconvincingly—in my view wrongly—overturned on appeal by the Supreme Court in *Suresh Koushal* vs *Naz Foundation* (2014) 1 SCC 1.

These and other failures suggest Indian privacy law has not matured to protect individual sovereignty, especially against the depredations of society and the state, which purport to enforce the morals of the community. For instance, there are currently concerted legislative and judicial attempts to prohibit an individual's right to privately view obscene content (*Kamlesh Vaswani* vs *Union of India* (2013), a freedom long upheld elsewhere under an implied right of privacy, such as in the US case of *Stanley* vs *Georgia*. In a similar vein, banning the private consumption of certain foods on grounds unrelated to safety, for instance the bans of beef and pork, negates the decisional autonomy of an individual's private right to eat. Although this claim has not been successfully advanced in India yet, it is being argued in the Bombay High Court in *Haresh Jagtiani* vs *State of Maharashtra* (2015).

Information Privacy

The fourth and final privacy claim, which is relatively recent in India, is made in relation to personal information. Personal information is that which can cause the identification of a person, whether used directly or in conjunction with other information. Personal information is required by the state to provide governance and is sought by commercial entities, both public and private, in order to provide goods and services. Information privacy law seeks to regulate the collection, use, storage, disclosure and destruction of personal information in order to protect the agency and expectations of the individuals to whom that information pertains.

State authorities have long collected personal information for the general purpose of governance, such as the decadal Census of India; or to issue identification documents, the production of which are a condition precedent to access many services and freedoms, such as ration cards, driver's licences, passports, electoral photo identity cards, and others. The latter documents serve the unwritten dual purpose of establishing identity in everyday life. State collections of personal information went unopposed for decades before the creation of the Aadhaar scheme in early 2009 to collect and store biometric information of all people resident in India. The Aadhaar scheme is consensual, no forcible collection of biometric information is provided for; and, the Supreme Court has temporarily disallowed condition precedential demands for Aadhaar cards to access government services in two orders of 23 September 2013 and 16 March 2015 in *Justice K S Puttaswamy* vs *Union of India* (2012). Nevertheless, privacy concerns regarding the security of the centralised database and the sharing of personal information remain, in addition to serious procedural infirmities stemming from the absence of an enabling statute (Greenleaf 2010).

On the other hand, a 2004 amendment to the Citizenship Act, 1955 permits the compulsory registration of citizens to enable the creation of the National Population Register (NPR), which also seeks biometric information, namely fingerprints and iris recognition scans. The NPR is the first countrywide biometric information collection effort, but there have long existed provisions in Indian criminal law to permit the forcible collection of fingerprints for forensic uses in certain cases. Section 73 of the Indian Evidence Act, 1872 permits such a collection of fingerprints, as does the Identification of Prisoners Act, 1920 which was further amended by Tamil Nadu in 2010 to enable the collection of blood samples. Indeed it is a common practice in most countries to forcibly collect fingerprints during the criminal justice process; therefore privacy interests demand the conditions that trigger forcible collection are reasonable to safeguard against capricious or arbitrary exercises of power.

Commercial collections of personal information have been largely unregulated in India despite the advance of information privacy law in Europe and other parts of the world. With the expansion of India's data processing industry, fuelled in large part by incoming personal information from Europe, pressure mounted on India to introduce legislation to comply with the outsourcing requirements of European privacy law (Greenleaf 2011a). In 2010, a European-commissioned assessment of Indian data privacy laws revealed large gaps in protective coverage to necessitate corrective action (Greenleaf 2011b). This remediation was dual: on the one hand the Department of Information Technology (DEITY) in the Ministry of Communications issued rules to institute a basic data protection regime (the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011), and on the other hand the Department of Personnel and Training (DOPT) in the Ministry of Personnel, Public Grievances and Pensions began drafting a comprehensive privacy bill.

The anomaly of two ministries in the same government attempting to make law on the same field appears to have been lost on observers. Law ought to be clear, but DEITY's rules were carelessly drafted prompting the department to issue a press clarification a few months later which in turn was dubious since law cannot be made or interpreted by press releases. In parallel, one year earlier, the DOPT had issued a white paper for privacy legislation where it counter-intuitively claimed: "India is not a particularly private nation" (Department of Personnel and Training 2010). Inchoate claims of this nature suggest tension between communitarian values and individual rights (Etzioni 1999, Etzioni 2000, Walzer 1990); they strike at the heart of the liberal construction of the citizen as an autonomous rights-bearer free from

the impositions of society and the state. Nevertheless, the resultant draft privacy bill was considered by a Committee of Secretaries in May 2011 whereupon it was returned to the DoPT for substantial modifications. The latest avatar of the bill has not been publicly released for comments yet, so a discussion of its merits would be premature.

Future Tense

If they receive sustained legislative or judicial attention, these four categories of privacy claims could form the basis for the creation of a coherent corpus of Indian privacy law. Such a law need not be omnibus, as the DoPT's first draft bill was in 2011. Indeed, the multiplicity of privacy claims, the diversity of the attendant legal principles, and the various challenges of enforcement would muddy the waters of any possible omnibus legislation. In the first place, there is a difference between the *in rem* public right to privacy against society and the state and the private "bundle of rights" afforded in tort law and by actionable claims (Dhavan 1979). This fundamental distinction has been blurred on several occasions, including by the Supreme Court in *R Rajagopal*, to warrant a clear demarcation in future law. Further, the technical and commercial expertise required to regulate data protection bears little relation to the constitutional, criminal and administrative law concerns that govern surveillance, free speech or decisional autonomy. For these and other reasons it is best if the individual constituents of Indian privacy law are left to mature in their silos.

However, there is a larger dissonance in Indian privacy jurisprudence that requires resolution before actual progress can be achieved. This is twofold. On the one hand, past privacy case law has failed to achieve theoretical clarity, and as a result a jumble of contending concepts confuses the law instead of substantiating it. For instance, in the *Gobind* case, which dealt with the limits of police surveillance on private property, the Supreme Court devoted most of its judgment to studying the emerging American ideal of decisional autonomy, which is chiefly concerned with protecting intangible choices rather than property. Yet, after having approved decisional autonomy, the Court abjectly failed to apply it when legitimately called upon to do so in the *Suresh Koushal* case. To use a litigator's yardstick, there is no test for privacy; no Indian judge has fashioned a judicial model of privacy that is logical, predictable, and supported by reason, not even the inimitable Justice Subba Rao whose contribution to privacy law continues to tower over the field.

On the other hand, as long as India's law and polity remain ambivalent about the rights of the individual against the community, privacy law will suffer. By whatever term the law employs to describe the undefined claims of the community—public interest, public morality, public order, or national security—the price of frequently privileging these claims over the freedoms of the individual is the loss of privacy. Since government policy has historically favoured homogenised notions of state interest and public order that imagine no space for privacy, an unwavering stand in favour of individual freedoms and privacy from interference by the community and state must be judicially taken by the constitutional courts

NOTES

1 House of Lords Debates (HL Deb) 13 March 1961, Vol 229, cc 607–61 and HL Deb, 15 June 1961, Vol 232, cc 289–99.

2 *Gazette of India* 12 March 1898, part V, p 212 and *Gazette of India* 26 March 1898, part VI, pp 285–287.

REFERENCES

Allen, Anita (1988): *Uneasy Access: Privacy for Women in a Free Society*, Totowa: Rowman & Littlefield.

Alshech, Eli (2007): "Out of Sight and Therefore Out of Mind: Early Sunni Islamic Modesty Regulations and the Creation of Spheres of Privacy," *Journal of Near Eastern Studies*, 66(4): 267–90.

Arun, Chinmayi (2014): "Filtering Content on the Internet," *Hindu*, 2 May.

Borges, Jorge Luis (1985): *Dreamtigers*, Austin: University of Texas Press.

Clark, R H (1974): "Constitutional Sources of the Penumbral Right to Privacy, *Villanova Law Review*, 19(6): 833–84.

Cohen, Julie (2010): "The Inverse Relationship between Secrecy and Privacy, *Social Research*, 77(3): 883–98.

Cooley, Thomas McIntyre (1888): *A Treatise on the Law of Torts*, Chicago: Callaghan.

De Bruin, Boudewijn (2010): "The Liberal Value of Privacy," *Law and Philosophy*, 29(5): 505–34.

Department of Personnel and Training (2010): "Approach Paper for a Legislation on Privacy," Government of India, viewed on 29 April 2015, (http://www.prsindia.org/theprsblog/wp-content/uploads/2011/06/aproach_paper.pdf).

Dhavan, Rajeev (1979): "Privacy: Adventures of a Concept," *Indian Journal of Comparative Law*, 19–48.

— (2008): *Publish and Be Damned*, New Delhi: Tulika.

Emerson, Thomas (1979): "The Right of Privacy and Freedom of the Press," *Harvard Civil Rights-Civil Liberties Law Review*, 14(2): 329–60.

Etzioni, Amitai (1999): *The Limits of Privacy*, New York: Basic Books.

— (2000): "A Communitarian Perspective on Privacy," *Connecticut Law Review*, 32(3): 897–905.

Fried, Charles (1968): "Privacy," *The Yale Law Journal*, 77 (3): 475–93.

Gavison, Ruth (1980): "Privacy and the Limits of Law," *The Yale Law Journal*, 89(3): 421–71.

— (1992): "Feminism and the Public/Private Distinction," *Stanford Law Review*, 45(1): 1–45.

Gerstein, Robert (1978): "Intimacy and Privacy," *Ethics*, 89(1), 76–81.

Goldring, John (1984): "Privacy and Property," *The Australian Quarterly*, 56(4), 308–24.

Government of India (1982): "Report of the Second Press Commission," Vols 1–2, New Delhi: Government Press.

Greenleaf, Graham (2010): "India's National ID System: Danger Grows in a Privacy Vacuum", *Computer Law and Security Review*, 26(5): 479–91.

— (2011a): "India's U-Turns on Data Privacy," *Privacy Laws & Business International Report*, Issues 110–114: UNSW Law Research Paper No 2011–42.

— (2011b): "Promises and Illusions of Data Protection in Indian Law, *International Data Privacy Law*, 1(1): 47–69.

Habermas, Jürgen (1991): *The Structural Transformation of the Public Sphere*, Cambridge: MIT Press.

Inness, Julie (1991): "Information, Access, or Intimate Decisions about One's Actions? The Content of Privacy," *Public Affairs Quarterly*, 5(3): 227–42.

Lane, Frederick S (2009): *American Privacy: The 400-Year History of Our Most Contested Right*, Boston: Beacon Press.

Lessig, Lawrence (2002): "Privacy as Property, *Social Research*, 69(1), 247–69.

Litman, Jessica (2000): "Information Privacy/Information Property, *Stanford Law Review*, 52 (5): 1283–1313.

Locke, John (1689): *Two Treatises of Government* (London).

MacKinnon, Catharine A (1989): *Toward a Feminist Theory of the State*, Cambridge: Harvard University Press.

Markesinis, Basil; Colm O'Cinneide, Jörg Fedtke and Myriam Hunter-Henin (2004): "Concerns and Ideas about the Developing English Law of Privacy (And How Knowledge of Foreign Law Might be of Help)," *The American Journal of Comparative Law*, 52(1): 133–208.

McCloskey, H J (1974): "Liberalism," *Philosophy*, 49(187): 13–32.

— (1980): "Privacy and the Right to Privacy," *Philosophy*, 55(211): 17–38.

Mill, John Stuart (1859): *On Liberty*, London: John W Parker and Son.

Ministry of Law (1968): "Thirty-Eighth Report of the Law Commission of India: Indian Post Office Act, 1898," New Delhi: Government of India.

Moore, Adam M (1998): "Intangible Property: Privacy, Power, and Information Control, *American Philosophical Quarterly*, 35(4): 365–78.

Neill, Brian (1962): "The Protection of Privacy," *Modern Law Review*, 25(4): 393–405.

Neocleous, Mark (2002): "Privacy, Secrecy, Idiocy, *Social Research*, 69(1): 85–110.

Nissenbaum, Helen (2004): "Privacy as Contextual Integrity," *Washington Law Review*, 79(1): 119–58.
— (2010): *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Palo Alto: Stanford University Press.
— (2011): "A Contextual Approach to Privacy Online," *Daedalus*, 140(4): 32–48.
Noorani, A G (2011): "A Case for Privacy," *Frontline*, 28(24), 19 November.
O'Brien, David M (1979): *Privacy, Law, and Public Policy*, New York: Praeger.
Posner, Richard (1979): "Privacy, Secrecy, and Reputation," *Buffalo Law Review*, 28: 1–55.
Post, Robert C (1989): "The Social Foundations of Privacy: Community and Self in Common Law Tort," *California Law Review*, 77(5): 957–1010.
Pow, Choon-Piew (2009): *Gated Communities in China: Class, Privilege and the Moral Politics of the Good Life*, Abingdon: Routledge.
Pratt, Walter F (1979): *Privacy in Britain*, London, New Jersey: Associated University Presses.
Prosser, William (1960): "Privacy," *California Law Review*, 48 (3): 383–423.
Rahman, M (1994): "A Loaded Bill," *India Today* (31 July 1994), viewed on 28 April 2015 (http://indiatoday.intoday.in/story/another-attempt-to-muzzle-the-press/1/293731.html).
Rawls, John (1971): *A Theory of Justice*, Cambridge: Harvard University Press.
Rössler, Beate (2005): *The Value of Privacy*, Cambridge: Polity Press.
Schoeman, Ferdinand (1984): "Privacy: Philosophical Dimensions of the Literature", *Philosophical Dimensions of Privacy: An Anthology* in Schoeman, Ferdinand (ed), Cambridge: Cambridge University Press.
Seipp, David J (1983): "English Judicial Recognition of a Right to Privacy," *Oxford Journal of Legal Studies*, 3(3): 325–370.
Shakespeare, William: *As You Like It*, Act II, Scene VII: 139–166.
Solove, Daniel (2002): "Conceptualizing Privacy," *California Law Review*, 90 (4): 1087–1155.
Solove, Daniel (2006): "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, 154(3): 477–560.
Walzer, Michael (1990): "The Communitarian Critique of Liberalism," *Political Theory*, 18(1): 6–23.
Warren, Samuel and Louis Brandeis (1890): "The Right to Privacy," *Harvard Law Review*, 4(5): 193–220.
Westin, Alan (1967): *Privacy and Freedom*, New York: Athenum.
Zarrow, Peter (2012): "The Origins of Modern Chinese Concepts of Privacy: Notes on Social Structure and Moral Discourse" in McDougall, Bonnie and Anders Hansson (eds), *Chinese Concepts of Privacy*, Leiden, Boston, Köln: Brill.

Case Laws Referred

R Rajagopal vs *State of Tamil Nadu* (1994) 6 SCC 632.
S A S vs *France* (Application 43835/11) 2014.
Virgil vs *Time, Inc* 527 F.2d 1122 (1975).
Campbell vs *Mirror Group Newspapers* [2004] UKHL 22.
Mosley vs *News of the World* [2008] EWHC 1777 (QB).
Von Hannover vs *Germany* (Application 59320/00).
Time, Inc vs *Hill* 385 US 374.
Welling vs *Weinfeld* 866 N E 2d 1051 (Ohio 2007).
Anderson vs *Gannett Company* 994 So2d 1048 (Fla 2008).
Wainwright vs *Home Office* [2003] 3 All ER 943.
A vs *B plc* [2003] QB 195.
Douglas vs *Hello!* [2003] EWHC (Ch) 786.
Ellis vs *Chief Constable Essex Police* [2003] EWHC 1321.
R Rajagopal vs *State of Tamil Nadu* (1994) 6 SCC 632.
Ratan Tata vs *Union of India* WP (Civil) 398 of 2010.
Weeks vs *United States* 232 US 383.
Kuruma, son of Kaniu vs *R* (1955) 1 All ER 236 (PC).
RM Malkani vs *State of Maharashtra* AIR 1973 SC 157
Olmstead vs *United States* 277 US 438.
Katz vs *United States* 389 US 347.
People's Union for Civil Liberties (PUCL) vs *Union of India* (1997) 1 SCC 301.
Maneka Gandhi vs *Union of India* (1978) 1 SCC 248.
Kharak Singh vs *State of Uttar Pradesh* (1964) 1 SCR 332.
Gobind vs *State of Madhya Pradesh* (1975) 2 SCC 148.
State vs *Navjot Sandhu* (2005) 11 SCC 600.
Griswold vs *Connecticut* 381 US 479.
Roe vs *Wade* 410 US 113.
Bowers vs *Hardwick* 478 US 186.
Lawrence vs *Texas* 539 US 558.
Naz Foundation vs *Government of NCT Delhi* 160 DLT 277 (2009).
Suresh Koushal vs *Naz Foundation* (2014) 1 SCC 1.
Kamlesh Vaswani vs *Union of India* WP (Crl) 177 of 2013.
Stanley vs *Georgia* 394 US 557.
Haresh Jagtiani vs *State of Maharashtra* WP (L) 982 of 2015.
Justice KS Puttaswamy vs *Union of India* WP(C) 494 of 2012.