National Law School of India Review

Volume 26 | Issue 2 Article 3

2014

State Surveillance and the Right to Privacy in India: A Constitutional Biography

Gautam Bhatia

NLSIR

STATE SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL BIOGRAPHY

Gautam Bhatia[1]

I. INTRODUCTION

Ever since the explosive Snowden disclosures in May 2013, State surveillance and citizens' right to privacy have been at the forefront of international debate. Even as the Snowden documents were revealing, detail by detail, the American and British intelligence agencies' extensive surveillance systems (PRISM and TEMPORA, among others) used to spy both on their own citizens, and upon communications elsewhere, reports about Indian bulk surveillance began to trickle in. It is now known that there are at least two surveillance regimes in India, in uncertain stages of preparation: the Central Monitoring System (CMS), which provides for the collection of telephony metadata by tapping into the telecommunications' companies records[2]; and Netra, a dragnet surveillance system that detects and sweeps up electronic communication that uses certain keywords such as "attack", "bomb", "blast" or "kill". These programs, wide in their reach and scope, have dubious statutory backing. They also, very clearly, impinge upon basic fundamental rights. A discussion of the legal and constitutional implications, therefore, is long overdue.

This essay presents an analytical and chronological history of the Indian Supreme Court's engagement with the right to privacy. While discussions for a privacy statute have stagnated and are presently in limbo[3], the Court has been active for nigh on fifty years. This essay aims to achieve a comprehensive, doctrinal understanding of the constitutional right to privacy, as evolved, understood and implemented by the judiciary. Such an understanding, indeed, is an essential

---

[1] Advocate, Delhi High Court.

[2] P. Munkaster, *India Introduces Central Monitoring System*, THE REGISTER, 8-5-2013, available at <http://www.theregister.co.uk/2013/05/08/india_privacy_woes_central_monitoring_system/> (last visited on 10-2-2015).

[3] Centre for Internet and Society, *An Analysis of the New Draft Privacy Bill*, MEDIANAMA, 28-3-2014, available at <http://www.medianama.com/2014/03/223-an-analysis-of-the-new-draft-privacy-bill-cis-india/> (last visited on 10-2-2015).

prerequisite to embarking upon a legal and constitutional critique of mass State surveillance in India.

II. FOUNDATIONS

Privacy is not mentioned in the Constitution. It plays no part in the Constituent Assembly Debates. Indeed, a proposal to include a provision akin to the American Fourth Amendment (and the root of American privacy law), prohibiting 'unreasonable searches and seizures', was expressly rejected by the Assembly. The place of the right – if it exists – must therefore be located within the structure of the Constitution, as fleshed out by judicial decisions.

The first case to address the issue was *M.P. Sharma* v. *Satish Chandra*[4] in 1954. In that case, the Court upheld search and seizure in the following terms:

> "A power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the Constitution makers have thought fit not to subject such regulation to Constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a totally different fundamental right by some process of strained construction." (emphasis supplied)

The right in question was Art. 19(1)(f) – the right to property. Notice here that the Court did not reject a right to privacy altogether – it only rejected it in the context of searches and seizures for documents, the specific prohibition of the American Fourth Amendment (that has no analogue in India). This specific position, however, would not last too long, and was undermined by the very next case to consider this question, *Kharak Singh*[5].

In *Kharak Singh* v. *State of U.P.*[6], the UP Police Regulations conferred surveillance power upon certain "*history sheeters*" – that is, those charged (though not necessarily convicted) of a crime. These surveillance powers included secret picketing of the suspect's house, domiciliary visits at night, enquiries into his habits and associations, and reporting and verifying his movements. These were challenged on Article 19(1)(d) (freedom of movement) and Article 21 (personal liberty) grounds. It is the second ground that particularly concerns us.

---

[4] AIR 1954 SC 300 ("*M.P. Sharma*").
[5] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[6] AIR 1963 SC 1295 : (1964) 1 SCR 332 ("*Kharak Singh*").

As a preliminary matter, we may observe that the Regulations in question were administrative – that is, they did not constitute a 'law', passed by the legislature. This *automatically* ruled out a 19(2) – 19(6) defence, and a 21 "*procedure established by law*" defence – which were only applicable when the State made a *law*. The reason for this is obvious: fundamental rights are extremely important. If one is to limit them, then that judgment must be made by a competent *legislature*, acting through the proper, deliberative channels of lawmaking – and not by mere administrative or executive action. Consequently – and this is quite apart from the question of administrative/executive *competence* – if the Police Regulations were found to violate Article 19 or Article 21, that made them *ipso facto* void, without the exceptions kicking in.

It is also important to note one other thing: as a defence, it was *expressly* argued by the State that the police action was reasonable and in the interests of maintaining public order precisely because it was *"directed only against those who were on proper grounds suspected to be of proved anti-social habits and tendencies and on whom it was necessary to impose some restraints for the protection of society."*[7] The Court agreed, observing that this would have *"an overwhelming and even decisive weight in establishing that the classification was rational and that the restrictions were reasonable and designed to preserve public order by suitable preventive action"*[8] – if there had been a law in the first place, which there wasn't. Thus, this issue itself was hypothetical, but what is crucial to note is that the State argued – and the Court endorsed – the basic idea that what makes surveillance reasonable under Article 19 is the very fact that it is *targeted* – targeted at individuals who are specifically suspected of being a threat to society because of a history of criminality.

Let us now move to the merits. The Court upheld secret picketing on the ground that it could not affect the petitioner's freedom of movement since it was, well, *secret*. What you don't know, apparently, cannot hurt you. What the Court found fault with was the intrusion into the petitioner's dwelling, and knocking at his door late at night to wake him up. The finding required the Court to interpret the meaning of the term "*personal liberty*" in Article 21. By contrasting the very specific rights listed in Article 21, the Court held that:

> "Is then the word "personal liberty" to be construed as excluding from its purview an invasion on the part of the police of the sanctity of a man's home and an intrusion into his personal security and his right to sleep which is the normal comfort and a dire necessity for human existence even as an animal? It might not be inappropriate to refer here to the words of the preamble to the Constitution that it is designed to "assure the

[7] *Kharak Singh*, AIR 1963 SC 1295, 1299 : (1964) 1 SCR 332, 339.
[8] *Kharak Singh*, AIR 1963 SC 1295, 1299 : (1964) 1 SCR 332, 339.

> dignity of the individual" and therefore of those cherished human value as the means of ensuring his full development and evolution. We are referring to these objectives of the framers merely to draw attention to the concepts underlying the constitution which would point to such vital words as "personal liberty" having to be construed in a reasonable manner and to be attributed that these which would promote and achieve those objectives and by no means to stretch the meaning of the phrase to square with any preconceived notions or doctrinaire constitutional theories."[9] (emphasis supplied)

A few important observations need to be made about this paragraph. The first is that it immediately follows the Court's examination of the American Fifth and Fourteenth Amendments, with their guarantees of "*life, liberty and property...*" and is, in turn, followed by the Court's examination of the American Fourth Amendment, which guarantees the protection of a person's houses, papers, effects etc from unreasonable searches and seizures. The Court's engagement with the Fourth Amendment is ambiguous. It admits that "*our Constitution contains no like guarantee...*", but holds that *nonetheless* "*these extracts* [from the 1949 case, *Wolf* v. *Colorado*[10]] *would show that an unauthorised intrusion into a person's home and the disturbance caused to him thereby, is as it were the violation of a common law right of a man – an ultimate essential of ordered liberty*", thus tying its own holding in some way to the American Fourth Amendment jurisprudence.

Crucially, however, *at this point*, American Fourth Amendment jurisprudence was *propertarian based* – that is, the Fourth Amendment was understood to codify – with added protection – the common law of trespass, whereby a man's property was held sacrosanct, and not open to be trespassed against. Four years later, in 1967, in Katz[11], the Supreme Court would shift its own jurisprudence, to holding that the Fourth Amendment protected zones where persons had a "*reasonable expectation of privacy*", as opposed to simply protecting listed items of property (homes, papers, effects etc). *Kharak Singh*[12] was handed down before *Katz*[13]. Yet the quoted paragraph expressly shows that the Court anticipated *Katz*[14], and in expressly grounding the Article 21 personal liberty right within the meaning of *dignity*, utterly rejected the propertarian-tresspass foundations that it might have had. To use a phrase invoked by later Courts – in this proto-privacy case, the Court already set the tone by holding it to attach to *persons*, not *places*.

---

[9] *Kharak Singh*, AIR 1963 SC 1295, 1302 : (1964) 1 SCR 332, 349.
[10] 93 L Ed 1782 : 338 US 25 (1949).
[11] *Katz* v. *United States*, 19 L Ed 2d 576 : 389 US 347 (1967).
[12] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[13] 19 L Ed 2d 576 : 389 US 347 (1967).
[14] 19 L Ed 2d 576 : 389 US 347 (1967).

While effectively finding a right to privacy in the Constitution, the Court expressly declined to frame it that way. In examining police action which involved tracking a person's location, association and movements, the Court upheld it, holding that "*the right of privacy is not a guaranteed right under our Constitution* and therefore *the attempt to ascertain the movements of an individual which* is merely a manner in which privacy *is invaded is not an infringement of a fundamental right guaranteed by Part III.*"[15] (emphasis supplied)

The "*therefore*" is crucial. Although not expressly, the Court virtually holds, in terms, that tracking location, association and movements does violate privacy, and only finds that constitutional because *there is no guaranteed right to privacy within the Constitution.* Yet.

In his partly concurring and partly dissenting opinion, Subba Rao, J. went one further, by holding that the idea of privacy was, in fact, contained within the meaning of Article 21: "*it is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty.*" Privacy he defined as the right to "*be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures.*"[16] On this ground, he held all the surveillance measures unconstitutional.

Justice Subba Rao's opinion also explored a proto-version of the chilling effect. Placing specific attention upon the word "*freely*" contained within 19(1)(d)'s guarantee of free movment, Justice Subba Rao went specifically against the majority, and observed:

> "The freedom of movement in clause (d) therefore must be a movement in a free country, i.e., in a country where he can do whatever he likes, speak to whomsoever he wants, meet people of his own choice without any apprehension, subject of course to the law of social control. The petitioner under the shadow of surveillance is certainly deprived of this freedom. He can move physically, but he cannot do so freely, for all his activities are watched and noted. The shroud of surveillance cast upon him perforce engender inhibitions in him and he cannot act freely as he would like to do. We would, therefore, hold that the entire Regulation 236 offends also Art. 19(1)(d) of the Constitution."[17] (emphasis supplied)

[15] *Kharak Singh*, AIR 1963 SC 1295, 1303 : (1964) 1 SCR 332, 334.
[16] *Kharak Singh*, AIR 1963 SC 1295, 1306 : (1964) 1 SCR 332, 360 (Subba Rao, J. dissenting).
[17] *Kharak Singh*, AIR 1963 SC 1295, 1306 : (1964) 1 SCR 332, 361.

This early case, therefore, has all the aspects that plague mass surveillance today. What to do with administrative action that does not have the sanction of law? What role does targeting play in reasonableness – assuming there is a law? What is the philosophical basis for the implicit right to privacy within the meaning of Article 21's guarantee of personal liberty? And is the chilling effect a valid constitutional concern?

III. GOBIND AND THE COMPELLING STATE INTEREST TEST

After its judgment in *Kharak Singh*[18], the Court was not concerned with the privacy question for a while. The next case that dealt – peripherally – with the issue came eleven years later. In *R.M. Malkani* v. *State of Maharashtra*[19], the Court held that attaching a recording device to a person's telephone did not violate Section 25 of the Telegraph Act[20], because:

> "where a person talking on the telephone allows another person to record it or to hear it, it can-not be said that the other person who is allowed to do so is damaging, removing, tampering, touching machinery battery line or post for intercepting or acquainting himself with the contents of any message. There was no element of coercion or compulsion in attaching the tape recorder to the telephone."[21]

Although this case was primarily about the admissibility of evidence, the Court also took time out to consider – and reject – a privacy-based Article 21 argument, holding that:

> "Article 21 was invoked by submitting that the privacy of the appellant's conversation was invaded. Article 21 contemplates procedure established by law with regard to deprivation of life or personal liberty. The telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high handed interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants. It must not be understood that the Courts will tolerate safeguards for the protection of the citizen to be imperiled by permitting the police to proceed by unlawful or irregular methods."[22]
>
> (emphasis supplied)

---

[18] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[19] (1973) 1 SCC 471, 476 ("*R.M. Malkani*").
[20] S. 15, Indian Telegraph Act, 1885.
[21] *R.M. Malkani*, (1973) 1 SCC 471, 476.
[22] *R.M. Malkani*, (1973) 1 SCC 471, 479.

Apart from the fact that it joined *Kharak Singh*[23] in refusing to *expressly* find a privacy right within the contours of Article 21, there is something else that unites *Kharak Singh*[24] and *R.M. Malkani*[25]: the hypothetical in *Kharak Singh*[26] became a reality in *R.M. Malkani*[27]. What saved the telephone tapping precisely because it was directed at "... *a guilty person*", with the Court specifically holding that the laws were not for targeting innocent people. Once again, then, the *targeted* and *specific* nature of interception became a crucial – and in this case, a decisive – factor. One year later, in another search and seizure case, *Pooran Mal* v. *Director of Inspection (Investigation)*[28], the Court cited *M.P. Sharma*[29] and stuck to its guns, refusing to incorporate the Fourth Amendment into Indian Constitutional law.

It is *Gobind* v. *State of M.P.*[30], decided in 1975, that marks the watershed moment for Indian privacy law in the Constitution. Like *Kharak Singh*[31], *Gobind*[32] also involved domiciliary visits to the house of a history-sheeter. Unlike *Kharak Singh*[33], however, in *Gobind*[34] the Court found that the Regulations *did* have statutory backing – Section 46(2)(c) of the Police Act[35], which allowed State Government to make notifications giving effect to the provisions of the Act, one of which was the prevention of commission of offences. The surveillance provisions in the impugned regulations, according to the Court, were indeed for the purpose of preventing offences, since they were specifically aimed at repeat offenders. To that extent, then, the Court found that there existed a valid 'law' for the purposes of Articles 19 and 21.

By this time, of course, American constitutional law had moved forward significantly from eleven years ago, when *Kharak Singh*[36] had been decided. The Court was able to invoke *Griswold* v. *Connecticut*[37] and *Roe* v. *Wade*[38], both of which had found 'privacy' as an "*interstitial*" or "*penumbral*" right in the American Constitution – that is, not reducible to any one provision, but implicit in a number of separate provisions taken together. The Court ran together a

---

[23] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[24] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[25] (1973) 1 SCC 471.
[26] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[27] (1973) 1 SCC 471.
[28] (1974) 1 SCC 345.
[29] AIR 1954 SC 300.
[30] (1975) 2 SCC 148 ("*Gobind*").
[31] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[32] (1975) 2 SCC 148.
[33] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[34] (1975) 2 SCC 148.
[35] S. 46(2)(*c*), Police Act, 1861.
[36] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[37] 14 L Ed 2d 510 : 381 US 479 (1965).
[38] 35 L Ed 2d 147 : 410 US 113 (1973).

number of American authorities, referred to Locke and Kant, to dignity, to liberty and to autonomy, and ended by holding, somewhat confusingly:

> "... the right to privacy must encompass and protect the personal intimacies of the home, the family marriage, motherhood, procreation and child rearing. This catalogue approach to the question is obviously not as instructive as it does not give analytical picture of that distinctive characteristics of the right of privacy. Perhaps, the only suggestion that can be offered as unifying principle underlying the concept has been the assertion that a claimed right must be a fundamental right implicit in the concept of ordered liberty... there are two possible theories for protecting privacy of home. The first is that activities in the home harm others only to the extent that they cause offence resulting from the mere thought that individuals might he engaging in such activities and that such 'harm' is not Constitutionally protective by the state. The second is that individuals need a place of sanctuary where they can be free from societal control. The importance of such a sanctuary is that individuals can drop the mask, desist for a while from projecting on the world the image they want to be accepted as themselves, an image that may reflect the values of their peers rather than the realities of their natures... the right to privacy in any event will necessarily have to go through a process of case-by-case development."[39] (emphasis supplied)

But if no clear principle emerges out of the Court's elucidation of the right, it was fairly unambiguous in stressing the importance of the right itself. Interestingly, it grounded the right within the context of the freedom struggle. "*Our founding fathers*," it observed, "*were thoroughly opposed to a Police Raj even as our history of the struggle for freedom has borne eloquent testimony to it.*"[40] The parallels to the American Fourth Amendment are striking here: in his historical analysis Akhil Amar tells us that the Fourth Amendment was meant precisely to avoid the various abuses of unreasonable searches and seizures that were common in England at the time.[41]

The parallels with the United States become even more pronounced, however, when the Court examined the grounds for limiting the right to privacy. It held: "*Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right, that*

[39] *Gobind*, (1975) 2 SCC 148, 156.
[40] *Gobind*, (1975) 2 SCC 148, 157.
[41] Amar, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION (1998).

fundamental right must be subject to restriction on the basis of compelling public interest."[42] (emphasis supplied)

"*Compelling public interest*" is an interesting phrase, for two reasons. *First*, 'public interest' is a ground for fundamental rights restrictions under Article 19 (see, e.g., Article 19(6)), but the text of the Article 19 restrictions do not use – and the Court, in interpreting them, has not held – that the public interest must be "*compelling*". This suggests a stricter standard of review for an Article 21 privacy right violation than Article 19 violations. This is buttressed by the fact that in the same paragraph, the Court ended by observing: "*even if it be assumed that Article 19(5)* [restrictions upon the freedom of movement] *does not apply in terms, as the right to privacy of movement cannot be absolute, a law imposing reasonable restriction upon it for* compelling interest of State *must be upheld as valid.*"[43] (emphasis supplied) The Court echoes the language of 19(5), and *adds* the word "*compelling*". This surely cannot be an oversight.

More importantly – the compelling State interest is an American test, used often in equal protection cases and cases of discrimination, where 'suspect classes' (such as race) are at issue. Because of the importance of the right at issue, the compelling state interest test goes hand-in-hand with another test: *narrow tailoring.*[44] Narrow tailoring places a burden upon the State to demonstrate that its restriction is *tailored in a manner that infringes the right as narrowest manner that is possible to achieve its goals.* The statement of the rule may be found in the American Supreme Court case of *Grutter* v. *Bollinger*:

> "Even in the limited circumstance when drawing racial distinctions is permissible to further a compelling state interest, government is still constrained under equal protection clause in how it may pursue that end: the means chosen to accomplish the government's asserted purpose must be specifically and narrowly framed to accomplish that purpose."[45]

To take an extremely trivial example that will illustrate the point: the State wants to ban hate speech against Dalits. It passes legislation that bans "*all speech that disrespects Dalits.*" This is not narrowly tailored, because while all hate speech against Dalits necessarily disrespects them, all speech that disrespects Dalits is not necessarily hate speech. It was possible for the government to pass legislation banning only hate speech against Dalits, one that would have infringed upon free speech more narrowly than the "*disrespect law*", and still achieved its goals. The law is not narrowly tailored.

---

[42] *Gobind*, (1975) 2 SCC 148, 157.
[43] *Gobind*, (1975) 2 SCC 148, 158.
[44] *Grutter* v. *Bollinger*, 539 US 306, 333 (2003).
[45] *Grutter* v. *Bollinger*, 539 US 306, 333 (2003).

Crucially, then, the Court in *Gobind*[46] seemed to implicitly accept the narrow-tailoring flip side of the compelling state interest coin. On the constitutionality of the Police Regulations itself, it upheld their constitutionality *by reading them narrowly.* Here is what the Court said:

> "Regulation 855, in our view, empowers surveillance only of persons against whom reasonable materials exist to induce the opinion that they show a determination, to lead a life of crime – crime in this context being confined to such as involve public peace or security only and if they are dangerous security risks. Mere convictions in criminal cases where nothing gravely imperiling safety of society cannot be regarded as warranting surveillance under this Regulation. Similarly, domiciliary visits and picketing by the police should be reduced to the clearest cases of danger to community security and not routine follow-up at the end of a conviction or release from prison or at the whim of a police officer."[47] (emphasis supplied)

But Regulation 855 did not refer to the gravity of the crime at all. Thus, the Court was able to uphold its constitutionality only by *narrowing its scope in a manner that the State's objective of securing public safety was met in a way that minimally infringed the right to privacy.*

Therefore, whether the *Gobind*[48] bench was aware of it or not, its holding incorporates into Indian constitutional law and the right to privacy, *not just the compelling State interest test, but narrow tailoring as well.* The implications for surveillance systems such as the CMS and Netra are obvious. Because with narrow tailoring, the State must demonstrate that bulk surveillance of *all individuals*, whether guilty or innocent, suspected of crimes or not suspected of crimes (whether reasonably or otherwise), possessing a past criminal record or not, speaking to each other of breaking up the government or breaking up a relationship – *every bit of data* must be collected to achieve the goal of maintaining public security, and that *nothing narrower will suffice.* Can the State demonstrate this? Perhaps it can; but at the very least, it should be made to do so in open Court.

IV. THE PUBLIC/PRIVATE DISTINCTION, AND THE COURT'S WRONG TURN

We have seen that *Gobind*[49] essentially crystallized a constitutional right to privacy as an aspect of personal liberty, to be infringed only by a narrowly-tai-

[46] (1975) 2 SCC 148.
[47] *Gobind*, (1975) 2 SCC 148, 158.
[48] (1975) 2 SCC 148.
[49] (1975) 2 SCC 148.

lored law that served a compelling state interest. After the landmark decision in *Gobind*[50], *Malak Singh* v. *State of P&H*[51] was the next targeted-surveillance history-sheeter case to come before the Supreme Court. In that case, Rule 23 of the Punjab Police Rules was at issue. Its *vires* was not disputed, so the question was a direct matter of constitutionality. An order of surveillance was challenged by two individuals, on the ground that there were no reasonable bases for suspecting them of being repeat criminals, and that their inclusion in the surveillance register was politically motivated. After holding that entry into a surveillance sheet was a purely administrative measure, and thus required no prior hearing (*audi alteram partem*), the Court then embarked upon a lengthy disquisition about the scope and limitations of surveillance, which deserves to be reproduced in full:

> "... the police [do not] have a licence to enter the names of whoever they like (dislike?) in the surveillance register; nor can the surveillance be such as to squeeze the fundamental freedoms guaranteed to all citizens or to obstruct the free exercise and enjoyment of those freedoms; nor can the surveillance so intrude as to offend the dignity of the individual. Surveillance of persons who do not fall within the categories mentioned in Rule 23.4 or for reasons unconnected with the prevention of crime, or excessive surveillance falling beyond the limits prescribed by the rules, will entitle a citizen to the Court's protection which the court will not hesitate to give. The very rules which prescribe the conditions for making entries in the surveillance register and the mode of surveillance appear to recognise the caution and care with which the police officers are required to proceed. The note following R. 23.4 is instructive. It enjoins a duty upon the police officer to construe the rule strictly and confine the entries in the surveillance register to the class of persons mentioned in the rule. Similarly R.23.7 demands that there should be no illegal interference in the guise of surveillance. Surveillance, therefore, has to be unobstrusive and within bounds. Ordinarily the names of persons with previous criminal record alone are entered in the surveillance register. They must be proclaimed offenders, previous convicts, or persons who have already been placed on security for good behaviour. In addition, names of persons who are reasonably believed to be habitual offenders or receivers of stolen property whether they have been convicted or not may be entered. It is only in the case of this category of persons that there may be occasion for abuse of the power of the police officer to make entries in the surveillance register. But, here, the entry can only be made by the order of

[50] (1975) 2 SCC 148.
[51] (1981) 1 SCC 420.

> the Superintendent of Police who is prohibited from delegating his authority under Rule 23.5. Further it is necessary that the Superintendent of Police must entertain a reasonable belief that persons whose names are to be entered in Part II are habitual offenders or receivers of stolen property. While it may not be necessary to supply the grounds of belief to the persons whose names are entered in the surveillance register it may become necessary in some cases to satisfy the Court when an entry is challenged that there are grounds to entertain such reasonable belief." (emphasis supplied)

Three things emerge from this holding: *first*, the Court follows *Gobind*[52] in locating the right to privacy within the philosophical concept of individual *dignity*, found in Article 21's guarantee of personal liberty. *Secondly*, it follows *Kharak Singh*[53], *R.M. Malkani*[54] and *Gobind*[55] in insisting that the surveillance be targeted, limited to fulfilling the government's crime-prevention objectives, and be limited – not even to suspected criminals, but – repeat offenders or serious criminals. And *thirdly*, it leaves open a role for the Court – that is, *judicial review* – in examining the grounds of surveillance, if challenged in a particular case.

After *Malak Singh*[56], there is another period of quiet. *LIC* v. *Manubhai D. Shah*[57], in 1993, attributed – wrongly – to *Indian Express Newspapers* the proposition that Article 19(1)(a)'s free expression right included privacy of communications (*Indian Express* itself had cited a UN Report without incorporating it into its holding).[58]

Soon afterwards, *R. Rajagopal* v. *State of T.N.*[59] involved the question of the publication of a convicted criminal's autobiography by a publishing house; Auto Shankar, the convict in question, had supposedly withdrawn his consent after agreeing to the book's publication, but the publishing house was determined to go ahead with it. Technically, this wasn't an Article 21 case: so much is made clear by the very manner in which the Court frames its issues: the question is whether a citizen of the country can prevent another person from writing his biography, or life story.[60] The Court itself made things clear when it held that the right of privacy has two aspects: the *tortious* aspect, which provides damages for a breach of individual privacy; and the *constitutional aspect*, which protects privacy against

---

[52] (1975) 2 SCC 148.
[53] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[54] (1973) 1 SCC 471.
[55] (1975) 2 SCC 148.
[56] (1981) 1 SCC 420.
[57] (1992) 3 SCC 637.
[58] (1992) 3 SCC 637, 651.
[59] (1994) 6 SCC 632 ("*Rajagopal*").
[60] *Rajagopal*, (1994) 6 SCC 632, 639.

unlawful governmental intrusion. Having made this distinction, the Court went on to cite a number of American cases that were precisely about the right to privacy against governmental intrusion, and therefore – ideally – irrelevant to the present case[61]; and then, without quite explaining how it was using these cases – or whether they were relevant at all, it switched to examining the law of defamation. It would be safe to conclude, therefore, in light of the clear distinctions that it made, the Court was concerned in *Rajagopal*[62] about an action between private parties, and therefore, privacy in the context of tort law. Its confusing observations, however, were to have rather unfortunate effects, as we shall see.

We now come to a series of curious cases involving privacy and medical law. In *'X'* v. *Hospital 'Z'*[63], the question arose whether a Hospital that – in the context of a planned marriage – had disclosed the appellant's HIV+ status, leading to his social ostracism – was in breach of his right to privacy. The Court cited *Rajagopal*[64], but unfortunately failed to understand it, and turned the question into one of the *constitutional right to privacy, and not the private right.* Why the Court turned an issue between two private parties – adequately covered by the tort of breach of confidentiality – into an Article 21 issue is anybody's guess. *Surely* Article 21 – the right to life and personal liberty – is not horizontally applicable, because if it was, we might as well scrap the entire Indian Penal Code, which deals with exactly these kinds of issues – individuals violating each others' rights to life and personal liberty. Nonetheless, the Court cited *Kharak Singh*[65], *Gobind*[66] and Article 8 of the European Convention of Human Rights, further muddying the waters, because Article 8 – in contrast to American law – embodies a *proportionality test* for determining whether there has been an impermissible infringement of privacy. The Court then came up with the following observation:

> "Where there is a clash of two Fundamental Rights, as in the instant case, namely, the appellant's right to privacy as part of right to life and Ms. Akali's right to lead a healthy life which is her Fundamental Right under Article 21, the RIGHT which would advance the public morality or public interest, would alone be enforced through the process of Court, for the reason that moral considerations cannot be kept at bay."[67]

With respect, this is utterly bizarre. If there is a clash of two rights, then that clash must be resolved by referring to the *Constitution*, and not to the Court's

---

[61] *Rajagopal*, (1994) 6 SCC 632, 643.
[62] (1994) 6 SCC 632.
[63] (1998) 8 SCC 296.
[64] (1994) 6 SCC 632.
[65] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[66] (1975) 2 SCC 148.
[67] (1998) 8 SCC 296, 309.

opinion of what an amorphous, elastic, malleable, many-sizes-fit "*public morality*" says. The mischief caused by this decision, however, was replicated in *Sharda* v. *Dharmpal*[68], decided by the Court in 2003. In that case, the question was whether the Court could require a party who had been accused of unsoundness of mind (as a ground for divorce under the wonderfully progressive Hindu Marriage Act, 1956) to undergo a medical examination – and draw an adverse inference if she refused. Again, whether this was a case in which Article 21 ought to be invoked is doubtful; at least, it is arguable, since it was the Court making the order. Predictably, the Court cited from *'X'* v. *Hospital 'Z'*[69] extensively. It cited *Gobind*[70] (compelling State interest) *and* the ECHR (proportionality). It cited a series of cases involving custody of children, where various Courts had used a 'balancing test' to determine whether the best interests of the child overrode the privacy interest exemplified by the client-patient privilege. It applied this balancing test to the case at hand by balancing the 'right' of the petitioner to obtain a divorce for the spouse's unsoundness of mind under the HMA, vis-à-vis the Respondent's right to privacy.

In light of the above analysis, it is submitted that although the outcome in *'X'* v. *Hospital 'Z'*[71] and *Sharda* v. *Dharmpal*[72] might well be correct, the Supreme Court has misread what *Rajagopal*[73] actually held, and its reasoning is deeply flawed. Neither of these cases are Article 21 cases: they are private tort cases between private parties, and ought to be analysed under private law, as *Rajagopal*[74] itself was careful to point out. In private law, also, the balancing test makes perfect sense: there are a series of interests at stake, as the Court rightly understood, such as certain rights arising out of marriage, all of a private nature. In any event, whatever one might make of these judgments, one thing is clear: they are both logically and legally irrelevant to the *Kharak Singh*[75] line of cases that we have been discussing, which are to do with the Article 21 right to privacy *against the State.*

V. PUCL V. UNION OF INDIA

Let us return, now, to our paradigm cases of surveillance. In 1997, the Supreme Court decided *People's Union for Civil Liberties (PUCL)* v. *Union of India.*[76] This case is the most important privacy case after *Gobind*[77], and the

[68] (2003) 4 SCC 493.
[69] (1998) 8 SCC 296.
[70] (1975) 2 SCC 148.
[71] (1998) 8 SCC 296.
[72] (2003) 4 SCC 493.
[73] (1994) 6 SCC 632.
[74] (1994) 6 SCC 632.
[75] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[76] (1997) 1 SCC 301 ("*PUCL*").
[77] (1975) 2 SCC 148.

most important case for our purposes, that of studying surveillance. It therefore deserves very close study.

At issue in *PUCL*[78] was telephone tapping, which is – for obvious reasons – central to our enquiry. In *PUCL*[79], the constitutionality of Section 5(2) of the Telegraph Act was at issue. This Section reads:

> "On the occurrence of any public emergency, or in the interest of public safety, the Central Government or a State Government or any Officer specially authorised in this behalf by the Central Govt. or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of and offence, for reasons to be recorded in writing, by order, direct that any message clear of messages to or from any person or classes of persons, relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detailed, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order."[80]
>
> (emphasis supplied)

Section 5(2), therefore, gives rise to a number of issues. The first is the meaning of the terms "*public emergency*" and "*public safety*". The second is the meaning of the terms "*persons or class of persons*". And the third – and this was the core of the arguments in the *PUCL case*[81] – is the scope of the procedural safeguards required to make this section constitutionally legitimate. A close reading of the case, I suggest, places *PUCL*[82] firmly within the continuing tradition of *Kharak Singh*[83] and *Gobind*[84], in setting stringent safeguards upon infringements of privacy.

The first thing to note is whether Section 5(2) is relevant at all to the question of *bulk* surveillance, *a la* CMS and Netra. There are at least three reasons to suggest that it is not. *First*, the Indian Telegraph Act is an 1885 legislation, drafted at a time when bulk surveillance was unimaginable, and aimed at addressing a very different problem – interception of *individual* telegraphic messages for specific, short-term purposes. *Secondly*, the term "*persons or class of persons*" in Section

---

[78] (1997) 1 SCC 301.
[79] (1997) 1 SCC 301.
[80] S. 5(2), Indian Telegraph Act, 1885.
[81] (1997) 1 SCC 301.
[82] (1997) 1 SCC 301.
[83] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[84] (1975) 2 SCC 148.

5(2) is clearly indicative of *identifiable* individuals (or classes of individuals), and is not meant to include the citizenry as a whole. And *thirdly*, the Court's own guidelines militate against reading permission for bulk surveillance into the Act (I'll come to this later). Section 5(2), therefore, does not authorize bulk surveillance, and does not authorize the CMS or Netra.

That said, let us now examine the development of privacy law in the case. The Court held unambiguously that individuals had a privacy interest in the content of their telephone communications. It cited *Kharak Singh*[85], *Gobind*[86] and *Rajagopal*[87] for the proposition that privacy was a protected right under Article 21. Coming, then, to the all-important interpretation of "*public emergency*" and "*public safety*", the Court held – and, it is submitted, correctly – that the two phrases "*take their colour off each other*". It defined public safety as the state of safety or freedom from danger for the public at large, and argued that neither a public emergency nor public safety could be "*secretive*", but must be evident to the reasonable person.

There is an elementary reason why "public emergency" and "public safety" cannot be given widely divergent interpretations. This is because if the standard embodied by one was laxer than the standard embodied by the other, then the latter would become redundant: in other words, if "*public safety*" is interpreted more broadly than public emergency, then there would be no point to having the phrase "*public emergency*" at all, because any public emergency would *necessarily* be a matter of public safety. The two categories must therefore be non-overlapping, referring to different aspects, and requiring roughly the same standard to be attracted. This argument is buttressed by the fact that the Court required a proclamation of an Emergency via public notification: now if that procedural safeguard is required in one case (Emergency), but the government can simply get around it by doing the same thing (phone interception) under the guise of public safety then, once again, "*public emergency*" becomes an almost redundant category, something clearly beyond the expectation of the legislature. For "*public safety*" to have any teeth, therefore, it must refer to a specific situation of identifiable danger – and *not* a general, vague idea – perhaps – of containing potential terrorist threats.

This position is buttressed by the Court's citation of the Press Commission Recommendations, which used the phrases "*national security*", "*public order*" and "*investigation of crimes*"[88] the Press Commission also urged regular review, and expiry within three months, once again suggesting that what was contemplated was a *specific* response to a *specific* situation, one that would expire once the situation itself expired (this is in keeping with the *targeted-surveillance*

[85] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[86] (1975) 2 SCC 148.
[87] (1994) 6 SCC 632.
[88] *PUCL*, (1997) 1 SCC 301, 315.

focus that we have seen in *Kharak Singh*[89], *R.M. Malkani*[90], *Gobind*[91] and *Pooran Mal*[92]). The Commission also categorically ran together "*public emergency*" and "*public safety*", by holding that in the interests of public safety, the surveillance power should be exercised one month at a time, extendible if the emergency continued (as we have argued above, this makes sense).

After citing the Press Commission observations with approval, the Court then addressed the question of whether judicial review was necessary. Taking its cue from the English Interceptions Act of 1985, it held that it was not. The Central Government had the authority to make the rules governing the specific exercise of the interception power. Since it had not done so for all these years, however, the Court stepped in to fill the breach.

The Court's rules are extremely instructive in order to understand how surveillance and privacy interact with each other. Under Rules 2 and 4, the Court required that the communications to be intercepted be *specified* (Rule 2), and the *persons* and the *addresses* specified as well (Rule 4); this is a very familiar proscription against general warrants – see, e.g., the American Fourth Amendment – "*no Warrants shall issue, but upon* probable cause, *supported by Oath or affirmation, and* particularly describing the place to be searched, and the persons or things to be seized".[93] (emphasis supplied) The whole purpose of this part of the Fourth Amendment was to mitigate the evil – prevalent under British colonial rule – of general warrants, giving a blank cheque to colonial officials to conduct widespread, dragnet invasions of privacy, as happened in the landmark case of *Entick* v. *Carrington*.[94] Indeed, the Virginia Declaration of Rights[95], one of the precursors of the Fourth Amendment, recognized even more explicitly the dangers to liberty that general warrants embodied, and clearly made this an issue about containing untrammeled executive power, and subjecting it to the rule of law:

> "That general warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted."[96] (emphasis supplied)

---

[89] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[90] (1973) 1 SCC 471.
[91] (1975) 2 SCC 148.
[92] (1974) 1 SCC 345.
[93] Amendment IV, United States Constitution, 1792.
[94] (1765) 19 Howells' State Trials 1029 : 95 ER 807.
[95] Virginia Declaration of Rights, 1776.
[96] S. 10, Virginia Declaration of Rights, 1776.

Therefore, Rule 4, based as it is upon such lineage, clarifies beyond any doubt that Section 5(2) does not permit bulk, indiscriminate surveillance; because if it did, it would not make any sense to require specificity of disclosure for communication, persons and addresses. Once again, the idea is simple: the government must act on some reasonably strong suspicion before it begins to infringe citizens' privacy – it cannot simply do so on a general belief that at some point in the future the information it gleans might come in use; and it cannot intercept the data – and intrude upon the privacy of – *innocent* citizens, suspected of no wrongdoing.

Rules 3 and 7, read together, codify the narrow tailoring rule: Rule 3 requires the government to take into account whether "*the information which is considered necessary to acquire* could reasonably be acquired by other means." (emphasis supplied)[97] Rule 7 states: "*the use of intercepted material shall be limited to* the minimum that is necessary *in terms of Section 5(2) of the Act.*" (emphasis supplied)[98] The minimum necessary and reasonable acquisition by other means are a clear enunciation of the narrow tailoring rule, that requires the infringement of a right to be narrowly tailored to the legitimate State goal, and holds it invalid if that goal could be achieved in a manner that was less of an infringement upon the right in question.

What, then, are we to take away from *PUCL*[99]? In my view, three things:

(a) Neither the Telegraph Act nor the Court contemplates bulk surveillance. Consequently, the Court's specific view that *targeted* surveillance does not need judicial review is not necessarily true for *bulk* surveillance.

(b) Rigorous standards are needed to justify an infringement of privacy rights – in other words, a compelling State interest (although the Court does not use the specific term).

(c) Privacy restrictions must be narrowly tailored, if they are to be constitutional. This means that they must be targeted, based on specific suspicion of identifiable individuals (as opposed to a general dragnet sweep), and the only means possible to fulfill the government's goals of public safety and crime prevention. In both (b) and (c), therefore, the Court continues with the strong privacy-protection standards developed in *Gobind*[100], and afterwards.

---

[97] *PUCL*, (1997) 1 SCC 301, 317.
[98] *PUCL*, (1997) 1 SCC 301, 318.
[99] (1997) 1 SCC 301.
[100] (1975) 2 SCC 148.

And at the end of the day, it affirms one very basic thought: that for liberty to flourish, there is an aspect of all our lives that must remain private from the government.

VI. AFTER PUCL

We noted how *PUCL*[101] entrenches a compelling state interest/narrow tailoring test for infringements of privacy. Cases after *PUCL*[102] are a mixed bag. *Collector* v. *Canara Bank*[103], decided in 2005, is notable for containing the most detailed examination of the development of American law, as well as Indian law, on searches and seizures and the associated right to privacy. In that case, Section 73 of the Stamp Act, that allowed – *inter alia* – the Collector to access *private records* that would normally be subject to the confidentiality relationship between banker and customer, was challenged. The Court made two very important observations: responding to the contention that once one had voluntarily given over one's bank records to a third party, there was no privacy interest remaining in them (as held in the much-critcised American case of *United States* v. *Miller*[104]), the Court made an *obiter* observation in *Gobind*[105] the centerpiece of its holding:

> "... the right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in [sic] Bank, must continue to remain confidential vis-à-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank.... once that is so, then unless there is some probable or reasonable cause or reasonable basis or material before the Collector for reaching an opinion that the documents in the possession of the Bank tend to secure any duty or to prove or to lead to the discovery of any fraud or omission in relation to any duty, the search or taking notes or extracts therefore, cannot be valid. The above safeguards must necessarily be read into the provision relating to search and inspection and seizure so as to save it from any unconstitutionality."[106] (emphasis supplied)

Three things stand out: the first is an affirmation that the right is one that vests in *persons* (consequently, when we support this with the *PUCL*[107] holding, the privacy interest in phone data becomes inescapable); *secondly*, once again in line with all previous cases, the Court requires reasonable suspicion *before* the

---

[101] (1997) 1 SCC 301.
[102] (1997) 1 SCC 301.
[103] (2005) 1 SCC 496 ("*Canara Bank*").
[104] 48 L Ed 2d 71 : 425 US 435 (1976) ("*Miller*").
[105] (1975) 2 SCC 148.
[106] *Canara Bank*, (2005) 1 SCC 496, 523.
[107] (1997) 1 SCC 301.

surveillance in question (in this case, a search and seizure) is undertaken. Once again, then, there is a clear indication that anything more than a *targeted* search is *ipso facto* unreasonable. And *thirdly*, the Court reads down a provision to mean that in order to save it from unconstitutionality (as it read procedural safeguards into Section 5(2) Telegraph Act, and as it will hopefully do to the IT Act).

The Court's second holding is equally interesting:

> "Secondly, the impugned provision in sec. 73 enabling the Collector to authorize 'any person' whatsoever to inspect, to take notes or extracts from the papers in the public office suffers from the vice of excessive delegation as there are no guidelines in the Act... under the garb of the power conferred by Section 73 the person authorized may go on [sic] rampage searching house after house i.e. residences of the persons or the places used for the custody of documents. The possibility of any wild exercise of such power may be remote but then on the framing of Section 73, the provision impugned herein, the possibility cannot be ruled out."[108] (emphasis supplied)

This paragraph is critical, because for the first time, the Court rules that if the framing of the legislation leaves it open to an abuse of privacy rights, then the legislation is constitutionally problematic *even though* the possibility of abuse is remote. And this is what is *precisely* the problem with bulk surveillance – collecting the content of every citizens' communications reveals to the government (and, by extension, private contractors, to the extent they are involved) *everything* about your personal life. Your religious beliefs, your political views, what you watch on the internet, which restaurant you go to eat, your friends, workmates and lovers – one doesn't need so summon up an Orwellian dystopia to understand the vast possibility of abuse here, abuse that was not even contemplated by the judges in *Canara Bank*[109] who held Section 73 unconstitutional, abuse that is ripe for being inflicted upon dissidents and unpopular minorities, precisely the groups that a Constitution is most required to protect. It is submitted, therefore, that both aspects of the *Canara Bank*[110] holding make it extremely difficult to justify across-the-board bulk surveillance.

Following on from *Canara Bank*[111], in *P.R. Metrani* v. *CIT*[112], a search and seizure provision in the Income Tax Act (Section 132(5)) was construed strictly as it constituted a "*serious invasion into the privacy of a citizen.*" Similarly,

---

[108] *Canara Bank*, (2005) 1 SCC 496, 524.
[109] (2005) 1 SCC 496.
[110] (2005) 1 SCC 496.
[111] (2005) 1 SCC 496.
[112] (2007) 1 SCC 789.

Directorate of Revenue v. *Mohd. Nisar Holia*[113] involved the interpretation of the search and seizure provisions of Sections 42 and 43 of the NDPS Act. Citing both *Canara Bank*[114] and *Gobind*[115], the Court held that the right to privacy was crucial, and imposed a strict requirement of written recording of reasons (once again, notice the targeted nature of the search) before an NDPS search-and-seizure could be carried out.

In light of these cases, the Court's 2008 judgment in *State of Maharashtra* v. *Bharat Shanti Lal Shah*[116] must rank among the more disappointing opinions that the Court has handed down in an area in which its jurisprudence has been satisfactory, as a whole. *Bharat Shanti Lal Shah*[117] involved a constitutional challenge to Sections 13 – 16 of the Maharashtra Control of Organised Crime Act that, like *PUCL*[118], involved provisions for interception of telephone (and other wireless) communications. The Court dismissed the contention in a paragraph, refusing to take the trouble of a meaningful analysis:

> "The object of the MCOCA is to prevent the organised crime and a perusal of the provisions of Act under challenge would indicate that the said law authorizes the interception of wire, electronic or oral communication only if it is intended to prevent the commission of an organised crime or if it is intended to collect the evidence to [sic] the commission of such an organized crime. The procedures authorizing such interception are also provided therein with enough procedural safeguards, some of which are indicated and discussed hereinbefore."[119]

It is disappointing that the Court does not even refer to compelling State interest or narrow tailoring, although the underlined portion might hint at something of the sort. Nonetheless, if we scrutinize the impugned provisions closely, we can understand the kind of safeguards that the Court found satisfactory. Section 14, for example, requires details of the organized crime that "*is being committed*" or is "*about to be committed*" before surveillance may be authorized; the requirements include, in addition, a description of the "*nature and location of the facilities*" from which the communication is to be intercepted, the "*nature of the communication*" and, if known, "*the identity of the person.*" In addition, Section 14(2)(c) requires a "*statement as to whether or not other modes of enquiry or intelligence gathering have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous or is likely to expose the*

---

[113] (2008) 2 SCC 370.
[114] (2005) 1 SCC 496.
[115] (1975) 2 SCC 148.
[116] (2008) 13 SCC 5 ("*Bharat Shanti Lal Shah*").
[117] (2008) 13 SCC 5.
[118] (1997) 1 SCC 301.
[119] *Bharat Shanti Lal Shah*, (2008) 13 SCC 5, 28.

identity of those connected with the operation of interception."[120] Section 14(2)(d) requires special reasons for surveillance to continue after information has been received. An extension application, under Section 14(2)(f), requires an update on results thus far. Section 14(8) limits duration to sixty days, permitting extensions on specific grounds but only – again – for a period of sixty days, and requires "*minimal interception.*"

The attentive reader will note that this is – in terms – a codification of the *PUCL*[121] rules. Like *PUCL*[122], the focus of these rules is to prevent abuse through *specificity*: specificity of individuals and locations, specificity of duration of surveillance, specificity of reasons. Once again – and it almost no longer bears repeating – surveillance is tolerated only because of its narrow, targeted nature, a position further buttressed by the Section 14(2)(c) requirement of exhausting all other options that achieve the same goal without infringing upon privacy before actually resorting to interception. Thus, even though the *Bharat Shanti Lal Shah*[123] bench did not refer to compelling State interest and narrow tailoring, it is obvious that their upholding of MCOCA was predicated upon these considerations.

VII. THE THIRD PARTY DOCTRINE AND UNTIDY ENDNOTES

Canara Bank[124] departed from the American Supreme Court case of *Miller*[125] in basing privacy upon a *personal,* as opposed to *propertarian,* foundation ("*privacy is of persons, not places*"). *Miller*[126], however, also stood for an important proposition known as the 'third party doctrine', which has direct implications for the law of privacy in the context of the CMSection. It is crucial to examine *Miller*[127] in relation to *Canara Bank*[128] with respect to that. If *Canara Bank*[129] rejects the third-party doctrine, then this has profound implications for the constitutionality of CMS-surveillance; we must therefore pay close attention to the issue.

Before we commence, one distinction: there is a difference between telephone *tapping* (which *R.M. Malkani*[130] held as certainly violating a privacy interest), and telephone *records* that are held by telephone companies and are then turned over

[120] S. 14(2)(c), Maharashtra Control of Organised Crime Act, 1999.
[121] (1997) 1 SCC 301.
[122] (1997) 1 SCC 301.
[123] (2008) 13 SCC 5.
[124] (2005) 1 SCC 496.
[125] 48 L Ed 2d 71 : 425 US 435 (1976).
[126] 48 L Ed 2d 71 : 425 US 435 (1976).
[127] 48 L Ed 2d 71 : 425 US 435 (1976).
[128] (2005) 1 SCC 496.
[129] (2005) 1 SCC 496.
[130] (1973) 1 SCC 471.

to the government (the NSA's PRISM project, the GCHQ's Tempora Project, and our very own CMS). The third-party doctrine isn't applicable to *R.M. Malkani case*[131] of the government directly tapping your line, but becomes very important precisely when the information is routed to the government via a third party (in this case, the telecom companies). Since there is no settled case in India (to my knowledge) on CMS/PRISM style surveillance, we must examine the third-party doctrine as developed elsewhere.

Recall that in *Miller*[132], the question was whether a person had a privacy interest in *personal records* held by a bank. The Court held he did not, since:

> "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[133]
>
> (emphasis supplied)

This is known as the third-party doctrine. Speaking for four members of the Court in dissent, Justice Brennan rejected it, reasoning that:

> "[A] depositor reveals many aspects of his personal affairs, opinions, habits, associations. Indeed, the totality of bank records provides a virtual current biography. . . . Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds."[134]

Three years later, in *Smith* v. *Maryland*[135], the question arose whether a pen register (that is, an electronic device that records all numbers called from a particular telephone line), installed on the telephone's *company's* property, infringed upon a legitimate expectation of privacy. The Court held that it did not, because:

> "Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that

[131] (1973) 1 SCC 471.
[132] 48 L Ed 2d 71 : 425 US 435 (1976).
[133] *Miller*, 48 L Ed 2d 71 : 425 US 435, 443 (1976).
[134] *Miller*, 48 L Ed 2d 71 : 425 US 435, 451 (1976).
[135] 61 L Ed 2d 220 : 442 US 735 (1979).

> the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[136] (emphasis supplied)

Smith v. *Maryland*[137] is essentially the third-party doctrine applied to telephone records. Records in question are knowingly and voluntarily passed on to a third party (the telephone company), the customers being aware that the third party is storing and recording them. Consequently, there is no reasonable expectation of privacy. Of course, there is a gap in the logic: the fact that we have no reasonable expectation of privacy against the telephone company storing and recording our data does not mean that we have no reasonable expectation of privacy that *government* will not do so. Nonetheless, *Smith* v. *Maryland*[138] was what the government has relied upon in the recent NSA litigations across American District Courts. In the oral arguments in *ACLU* v. *Clapper*[139], which was the ACLU's challenge to NSA surveillance before the New York District Court[140], the government's entire privacy argument was based upon the *Smith* v. *Maryland*[141] holding, and ACLU's counter-arguments turned upon how, in the last thirty years, the use of the telephone had increased so much, with so many personal details now part of phone records, that *Smith*[142] no longer held the field.

Soon after the ACLU arguments, in November 2013, in *Klayman* v. *Obama*[143], Judge Leon at the Columbia District Court accepted in substance, the ACLU argument. He observed that "*the relationship between the police and phone company in* Smith *is nothing compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies*"[144] – that is, a formalized policy as opposed to a one-time collection. Judge Leon then went on to hold that not only was the government's surveillance technology vastly more all-encompassing than it had been in 1979, but also that "*the nature and quantity of information contained in peoples' telephony data is much greater as well.*"[145] The "*ubiquity*" of phones had altered both the amount of information available, and what that information could tell government about peoples' lives (and indeed, previously on the blog[146] we have discussed how bulk

---

[136] *Smith* v. *Maryland*, 61 L Ed 2d 220 : 442 US 735, 743 (1979).
[137] 61 L Ed 2d 220 : 442 US 735 (1979).
[138] 61 L Ed 2d 220 : 442 US 735 (1979).
[139] 959 F Supp 2d 724 (2014) (New York District Court).
[140] 959 F Supp 2d 724 (2014) (New York District Court) ("*ACLU*").
[141] 61 L Ed 2d 220 : 442 US 735 (1979).
[142] 61 L Ed 2d 220 : 442 US 735 (1979).
[143] 957 F Supp 2d 1 (2013) (Columbia District Court).
[144] *Klayman* v. *Obama*, 957 F Supp 2d 1, 38 (2013).
[145] *Klayman* v. *Obama*, 957 F Supp 2d 1, 39 (2013).
[146] *See* <https://indconlawphil.wordpress.com> (last visited on 28-1-2015).

surveillance of telephone records can enable government to construct a complete record of a person's social, sexual, religious and political mores). Consequently, Judge Leon held that there was likely to be a reasonable expectation of privacy in telephone records.

Does Canara Bank[147], in rejecting *Miller*[148], reject the third-party doctrine as well? I believe so, although not unambiguously. In the Court's mind, the third party doctrine is a corollary of the propertarian theory of privacy. Thus, in paragraph 54, the Court observes:

> "Once we have accepted in *Gobind*[149] and in latter cases that the right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in Bank, must continue to remain confidential vis-à-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank."[150] (emphasis supplied)

The Court here conflates "*no longer at the customer's house*" (persons v. places) and "*voluntarily sent to the Bank*" (third party). Because even if one holds that the right to privacy belongs to persons and not places, it is logically possible to hold that once one voluntarily turns over one's information to someone else, one no longer has a privacy interest in it. The Court, however, expressly forecloses that option by reading the two together – *because* the right of privacy belongs to persons and not to places, *therefore* we retain our privacy interests even in those documents that we have voluntarily turned over to a third party. In other words, the Court's logic appears to be that the *nature of the documents vis-à-vis us remains unchanged despite their location shifts from beyond our control, even if this shift is knowingly and voluntarily cause by us.* Thus, it would appear that *Canara Bank*[151] adopts a particular conception of privacy-interests-belong-to-peoples-and-not-places, one that rejects the third party doctrine. To repeat: this is not the only way in which we can understand the people/places distinction; conceptually, people/places and third-party come apart, as they have done so in American law. What we have tried to do here is to make sense of the *Canara Bank*[152] holding, and I submit that the only way to do so is to understand *Canara Bank*[153] as rejecting third party *through* one specific conception of people/places. Thus, the *Smith* v. *Maryland*[154] argument is not open to the government

---

[147] (2005) 1 SCC 496.
[148] 48 L Ed 2d 71 : 425 US 435, 443 (1976).
[149] (1975) 2 SCC 148.
[150] *Canara Bank*, (2005) 1 SCC 496, 523.
[151] (2005) 1 SCC 496.
[152] (2005) 1 SCC 496.
[153] (2005) 1 SCC 496.
[154] 61 L Ed 2d 220 : 442 US 735 (1979).

if it wishes to collect data from telecom companies or, in the case of the internet, ISPs. In light of *Canara Bank*[155], the privacy interest remains.

We may now end our substantive privacy law discussion by a brief examination of two cases whose locus lies in the domain of medical tests, although in differing areas. *Selvi* v. *State of Karnataka*[156], decided in 2010, involved the constitutionality of narco-analysis and polygraph tests during police investigations, and the testimonial statements obtained therefrom. The Court had no trouble in finding that, insofar as these techniques interfered with a person's mental processes in order to elicit information from him, they infringed his right to privacy. The Court then summarily rejected the State's argument of a compelling interest in eliciting information that could lead to the prevention of crime, holding that:

> "There is absolutely no ambiguity on the status of principles such as the 'right against self-incrimination' and the various dimensions of 'personal liberty'. We have already pointed out that the rights guaranteed in Articles 20 and 21 of the Constitution of India have been given a non-derogable status and they are available to citizens as well as foreigners. It is not within the competence of the judiciary to create exceptions and limitations on the availability of these rights."[157]
>
> (emphasis supplied)

This passage is curious. While a non-derogable right need not be an absolute right, our privacy jurisprudence suggests that the right to privacy is indeed derogable – when there is a compelling State interest. Insofar as *Selvi*[158] goes beyond the accepted doctrine, it is probably incorrectly decided; nonetheless, it affirms – once more – even if only through contentions made by the State, that the relevant standard for infringement is the compelling interest standard. Furthermore, in subsequently investigating whether compelled undertaking of narco-analysis or polygraph tests are *actually* likely to reveal the results that the investigating authorities need – and finding them unconstitutional because they don't – the Court takes a path that resembles narrow tailoring.

Lastly – and most recently – *Rohit Shekhar* v. *Narayan Dutt Tiwari*[159] dealt with a Court order requiring a compulsory DNA test in a paternity dispute. After lengthy citation of foreign precedent, the Court entered into a bewildering discussion of the relationship between DNA tests and the right to privacy. It held that *depending* upon the circumstances of a case, mandatory testing would be

---

[155] (2005) 1 SCC 496.
[156] (2010) 7 SCC 263 ("*Selvi*").
[157] *Selvi*, (2010) 7 SCC 263, 380.
[158] (2010) 7 SCC 263.
[159] 2011 SCC OnLine Del 4076 (Delhi High Court) ("*Rohit Shekhar*").

governed by a number of factors such as a compelling interest, a probable cause, decreased expectations of privacy, and so on. It then went on to hold:

> "forced interventions with an individual's privacy under human rights law in certain contingencies has been found justifiable when the same is founded on a legal provision ; serves a legitimate aim ; is proportional ; fulfils a pressing social need ; and, most importantly, on the basis that there is no alternative, less intrusive, means available to get a comparable result."[160]

This is extremely strange, because the first three conditions form part of a classic proportionality test; and the last two are – as readers will recognize – the two parts of the compelling state interest – narrow tailoring test. Indeed, the Court contradicts itself – "*legitimate aim*" and "*pressing social need*" cannot *both* be part of the test, since the latter makes the former redundant – a pressing social need will necessarily be a legitimate aim. Consequently, it is submitted that no clear ratio emerges out of *Rohit Shekhar*[161]. It leaves the previous line of cases – that we have discussed exhaustively – untouched.

VIII. CONCLUSION

Our enquiry has spanned fifty years and many different aspects of law that touch an individual's personal life – from criminal law practices (police surveillance, narco-analysis, self-incrimination) to phone-tapping, from marital relations to the status of one's bank records. Despite the diversity of cases and the differing reasoning employed by judges to reach differing results over time, we have seen that a careful analysis reveals certain unifying strands of logic and argument that can provide a coherent philosophical and constitutional grounding to the right to privacy in Indian law, bases that the Court can – and should – draw upon in order to decide an eventual CMS/bulk surveillance challenge in a principled manner.

We can commence by emphasizing the distinction between two sets of privacy cases, a distinction that the Court has failed to appreciate so far. One set of cases involves privacy claims *between private parties*. Examples include a hospital revealing a patient's medical records ('*X*' v. *Hospital 'Z'*[162]), or one spouse tapping the other's phone (*Rayala* v. *Rayala*[163]). Now, these cases involve the infringement of a privacy right, but they do so as a matter of *private law*, not *constitutional law*. As a matter of principle, the remedies would lie in tort – the tort of invasion of privacy, for instance, or breach of confidence. The Court's invocation of Article 21 in these cases must be deplored as a serious mistake. Article

[160] 2011 SCC OnLine Del 4076, para 79.
[161] 2011 SCC OnLine Del 4076.
[162] (1998) 8 SCC 296.
[163] AIR 2008 AP 98.

21 is sets out a constitutional right, and unless otherwise expressly provided by the Constitutional text (see, e.g., Article 15(2)), constitutional rights are applicable *vertically* against the State, and not *horizontally* between individuals. Once again, a simply hypothetical will illustrate the absurdity of cases like *Rayala*[164]: A murders B. Very obviously, the law governing this incident is the Indian Penal Code, which defines murder and prescribes the punishment for it. A has not violated B's Article 21 right to life by murdering him. Now, there is something to be said for philosophical arguments that challenge the public/private State/individual dichotomy as a matter of first principle. That, however, is not our concern here. Whatever the philosophical validity of the distinction, there is little doubt that our *Constitution* subscribes to it quite explicitly, by having a Part III in the first place, and with provisions such as Articles 13 and 32.

There is one way of reconciling these cases. That is to read them not as invoking Article 21 as a *ground for the decision*, but invoking it to infuse the right to privacy with *substantive content*. That is, the private law right to privacy and the constitutional right to privacy, while rooted in different sources and enforceable against different entities, nonetheless (reasonably enough) codify the same abstract conception of *what privacy is* – and it is to that end that the Court, in private-party cases, cites Article 21.

This is crucial, because it helps to clarify the way in which these two rights *are* different, and to make sense of a jurisprudence that would be hopelessly incoherent otherwise. The difference lies in the *standard for justifying an infringement*. In the private-party cases, the Court – rightly – treats the matter as balancing various rights and interests involved of the different parties to the case. *'X'* v. *Hospital 'Z'*[165], for instance – as understood by the Court – required a balancing of the patient's right to privacy against his future in-laws right to know about prior, debilitating medical records in order that there be informed consent to the marriage. Small wonder then, that in these cases the Court – again, rightly – cites Article 8 of the ECHR, and analyses them in the language of *proportionality*.

In cases involving the State, however, we have seen that the Court has (almost uniformly) insisted upon the far higher standard of *compelling State interest*. Again, there is a logic to this distinction. The importance of maintaining a private sphere against State intrusion, the extent to which the State now has the power to intrude (as we have all seen over the last six months), considerations that ultimately go to the heart of maintaining a free and democratic society – all justify (if not necessitate) a higher standard. Once we understand this, it is possible now to understand why the Supreme Court has adopted one test in some

[164] AIR 2008 AP 98.
[165] (1998) 8 SCC 296.

cases, and another test in other cases. The justification is a principled one (even if the Supreme Court might not have been aware of it).

Proceeding, then, to the Article 21 constitutional right to privacy. The Court has located this within Article 21's guarantee of personal liberty. In the early cases – *Kharak Singh*[166] and *Gobind*[167] – the Court understood the philosophical foundations of privacy to lie in the idea of individual dignity; that is, the basic thought that in order to live a dignified life, one must be able to have a sphere of action that is free from external invasion (this, essentially, is what is meant by the phrase, often used by the Court, "*the right to be left alone*"). The dignitarian justification of privacy is to be sharply contrasted with another justification, which held the field in American Constitutional law for a long while: the *propertarian* justification that grounds privacy in the idea that government is to keep off private property. This is what is meant by the Supreme Court's slogan, "*the right to privacy belongs to persons, not places.*"

Ultimately, possibly, the basic philosophy is similar – advocates for property rights argue that without a certain measure of private property, an individual cannot live an independent and dignified life. Practically, however, the shift encodes an analytical difference. A propertarian foundation – concretely – would involve a set of *spaces* that are placed out of bounds (e.g., the Fourth Amendment's list of "*homes, papers, effects*" etc.) The dignitarian foundation would extend its scope to *acts and places* with regard to which persons have a reasonable expectation of privacy. Naturally, this will – and has – led to different results in practice, with the dignitarian foundation leading to more expansive privacy protection.

The persons-not-places justification also led the Supreme Court to reject the third-party doctrine, according to which privacy interest is lost when personal effects are voluntarily handed over to a third party. In *Canara Bank*[168] the Court emphasized that the character of those items – their personal nature – does not change simply because their location has changed. The privacy interest is retained, whether they are bank records, or telephone details.

These are the contours of the privacy right. Naturally, it is not absolute, and the Court has taken pains to specify that on numerous occasions. What, then, justifies an infringement? The Court has consistently called for a "*compelling State interest*", one that rises beyond the simple "*public interest*" encoded in the Article 19 restrictions. Side-by-side with compelling State interest, the Court has also required – although it has never expressly spelt it out – the restrictive law to be *narrowly tailored.* In other words, the government must show that its infringing law not only achieves the compelling State interest, but does so in a way that restricts privacy in the narrowest possible manner. If there are other

[166] AIR 1963 SC 1295 : (1964) 1 SCR 332.
[167] (1975) 2 SCC 148.
[168] (2005) 1 SCC 496.

conceivable ways of achieving the same goal that do not infringe upon privacy to the extent the impugned law does, the law will be struck down. We see this in the police surveillance cases, where in *Gobind*[169], for instance, the Court read into Regulation 855 an additional requirement of gravity, to ensure that it was narrowly tailored; and we see it even more clearly in the phone-tapping cases, where the Court's rules require not only specification of persons, numbers and addresses, but also require the State to resort to surveillance only if other methods are not reasonably open, and in so doing, to infringe privacy minimally. Targeting, indeed, is critical: all the surveillance cases that we have explored have not only involved specific, targeted surveillance (indeed, Section 5(2) of the Telegraph Act only envisages targeted surveillance), but the very fact that the surveillance is targeted and aimed at individuals against whom there are more than reasonable grounds of suspicion, has been a *major – almost dispositive – ground* on which the Court has found the surveillance to be constitutional. Targeting, therefore, seems to be an integral aspect of narrow tailoring.

I do not mean to suggest that the above is a complete philosophical account of privacy. It ignores, for instance, the very legitimate concern that creating a private sphere only serves to justify relations of non-State domination and oppression within that sphere – both symbolically, and actually (see, for instance, the infamous marital rape exception in Indian criminal law). It presumes – instead of arguing for – the basic philosophical idea of the ultimate unit of society being indivisibly, atomized individual selves living in hermetically sealed 'zones' of privacy, an assumption that has come under repeated attack in more than fifty years of social theory. I hope to explore these arguments another day, but the purpose of this paper has been primarily doctrinal, not philosophical: to look at surveillance in the framework of established constitutional doctrine without questioning – at least for now – the normative foundations of the doctrine itself.

Our conclusions, then, summarized very briefly:

- the right to privacy is an aspect of Article 21's guarantee of personal liberty, and is grounded in the idea that a free and dignified life requires a private sphere
- one does not necessarily lose one's privacy interest in that which one hands over to a third party
- an infringement of privacy must be justified by a compelling state interest, and the infringing law must be narrowly tailored to serve that interest

As far as the CMS, Netra and other dragnet surveillance mechanisms go, it is clear, then, that they implicate a privacy interest; and to justify them, the

[169] (1975) 2 SCC 148.

government must show that there is no other way in which it could achieve its goals (of combating terrorism etc) without bulk surveillance on an industrial scale.

But if recent judgments of our Supreme Court do not exactly instill confidence in its role as the guarantor of our civil liberties[170], its long-term record in national security cases is even worse. *A.K. Gopalan*[171], *Habeas Corpus*[172] and the 2004 *People's Union for Civil Liberties* v. *Union of India*[173] come to mind as examples. It is therefore unclear how the Court will rule on a CMS/surveillance challenge. One thing is clear, though: the privacy law jurisprudence that it has developed over the last fifty years provide it with all the analytical tools to fulfil its constitutional mandate of protecting civil liberties. Consistent with the narrow tailoring test, the Supreme Court ought not to allow the government to baldly get away with asserting a national security interest, but require it to *demonstrate* not only how national security is served by dragnet surveillance, but also how dragnet surveillance is the *only* reasonable way of achieving national security goals. The possibility of abuse is too great, and the lessons that history teaches us – that totalitarianism always begins with pervasive governmental spying over individuals – is to be ignored at our peril.

In the meantime, privacy jurisprudence continues to explode worldwide. The end of 2013 witnessed the beginnings of the pushback against the American surveillance state. In his opinion on the Columbia Circuit Bench, which we referred to earlier, not only did Judge Leon hold the NSA spying program likely to be unconstitutional, but notably, he refused to accept NSA claims of national security on their face. He went into the record, and found that out of the 54 instances that the NSA had cited of allegedly foiled terrorist plots, it had miserably failed to prove *even one* where the outcome would have been different without bulk surveillance. This is a classic example of how narrow tailoring works. And later in the week, the Review Panel set up by President Obama emphatically rejected the contention that bulk surveillance is a necessary compromise to make in the liberty/security balance.[174] Nor is the United States alone; in June 2014, the Canadian Supreme Court handed down its decision in *R.* v. *Spencer*[175], where it prohibited the warrantless disclosure of basic subscriber information by internet companies, to law-enforcement agencies. The foundations of the Court's decision evidently included a rejection of the third-party doctrine, an expanded understanding of privacy, and the holding of the government to a high standard of proof before privacy could be violated 'in the interests of' law and order.

---

[170] *Suresh Kumar Koushal* v. *Naz Foundation*, (2014) 1 SCC 1.
[171] *A.K. Gopalan* v. *State of Madras*, AIR 1950 SC 27 : 1950 SCR 88.
[172] ADM, Jabalpur v. Shivakant Shukla, (1976) 2 SCC 521.
[173] (2004) 2 SCC 476.
[174] *Klayman* v. *Obama*, 957 F Supp 2d 1 (2013) (Columbia District Court).
[175] 2014 SCC 43 (Supreme Court of Canada).

Given all this, and given the worldwide pushback underway against such surveillance measures, from Brazil to Germany, it would be a constitutional tragedy if the Supreme Court ignored its own well-crafted jurisprudence and let the government go ahead with bulk surveillance on the basis of asserted and unproven national security claims. Tragic, but perhaps not entirely unexpected.