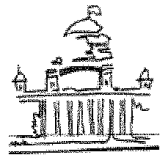

PAPER-THIN SAFEGUARDS AND MASS SURVEILLANCE IN INDIA

Chinmayi Arun[1]

The Indian government's new mass surveillance systems present new threats to the right to privacy. Mass interception of communication, keyword searches and easy access to particular users' data suggest that state is moving towards unfettered large-scale monitoring of communication. This is particularly ominous given that our privacy safeguards remain inadequate even for targeted surveillance and its more familiar pitfalls.

This need for better safeguards was made apparent when the Gujarat government illegally placed a young woman under surveillance for obviously illegitimate purposes[2], demonstrating that the current system is prone to egregious misuse. While the lack of proper safeguards is problematic even in the context of targeted surveillance, it threatens the health of our democracy in the context of mass surveillance. The proliferation of mass surveillance means that vast amounts of data are collected easily using information technology, and lie relatively unprotected.

This paper examines the right to privacy and surveillance in India, in an effort to highlight more clearly the problems that are likely to emerge with mass surveillance of communication by the Indian Government. It does this by teasing out our privacy rights jurisprudence and the concerns underpinning it, by considering its utility in the context of mass surveillance and then explaining the kind of harm that might result if mass surveillance continues unchecked.

The first part of this paper threads together the evolution of Indian constitutional principles on privacy in the context of communication surveillance as well as search and seizure. It covers discussions of privacy in the context of our

---

[1] Research Director of the Centre for Communication Governance at National Law University Delhi and Fellow of the Centre for Internet & Society, Bangalore. I thank Parul Sharma from National Law University Delhi for all her help with rounding up material for this paper.

[2] Several newspapers reported this. [*See* for example, *Fresh Tapes on Gujarat Government's Surveillance Emerge*, THE HINDU (Ahmedabad edition, 18-12-2013)]. By way of clarification, the law does not list anxieties of family members among the reasons for which surveillance may be conducted.

fundamental rights by the draftspersons of our constitution, and then moves on to the ways in which the Supreme Court of India has been reading the right to privacy into the constitution. The second part of this paper discusses the difference between mass surveillance and targeted surveillance, and international human rights principles that attempt to mitigate the ill effects of mass surveillance. The concluding part of the paper discusses mass surveillance in India, and makes a case for expanding our existing privacy safeguards to protect the right to privacy in a meaningful manner in face of state surveillance.

I. PRIVACY AND THE INDIAN CONSTITUTION

At the time of drafting of the Indian constitution, there were limited examples of codification of the right to privacy. Common law for instance did not have a clearly articulated privacy doctrine.[3] The European Convention on Human Rights, which contains one of the most powerful articulations of the right to privacy, was not in force at the time. However the United States of America used a patchwork of law to protect privacy in different contexts, and the principles from this law almost made its way into the Indian Constitution in the form of an amendment based on the US Fourth Amendment.

The Constituent Assembly did not take the right to privacy as seriously as it should have whilst crafting the Fundamental Rights. This might have been because of the relative scarcity of material on the right to privacy at the time. An amendment to insert the right against unreasonable searches was very nearly passed by the house, but ended up being dropped. This resulted in some initial reluctance on the part of the Supreme Court to read this right into the Constitution. However the Supreme Court of India did eventually read the right to privacy into the fundamental rights, and has been tracing out its contours through the different cases that implicate this right.

A. The Constituent Assembly and the Right to Privacy

Two different forms of privacy were proposed as insertions to the Fundamental Rights Chapter of the Constitution and both were rejected with very little debate. One of these was to do with safeguards against unreasonable search and the other protected the privacy of correspondence.

The amendment to embed safeguards against arbitrary search and seizure in the Indian Constitution was moved by Kazi Syed Karimuddin.[4] The proposed text read as follows:

---

[3] A.G. Noorani, *Right to Privacy*, 40(9) ECONOMIC AND POLITICAL WEEKLY 802 (26-2-2005).

[4] Amendment 512 moved by Kazi Syed Karimuddin, CONSTITUENT ASSEMBLY DEBATES, Volume VII, CONSTITUENT ASSEMBLY OF INDIA (3-12-1948).

> "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated and 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"[5]

Dr. Ambedkar was willing to accept Karimuddin's proposal.[6] He pointed out that this clause was already in the Criminal Procedure Code, and was therefore a part of Indian law, but also acknowledged that it may be desirable in the interests of personal liberty to '*place these provisions beyond the reach of the legislature*'.[7]

The chaos during voting over the proposal suggests that it was contentious. The Vice-President attempted twice to put the Karimuddin text to vote.[8] Although he declared the amendment as having been accepted both times, Mr. T.T. Krishnamachari objected, saying both times that the majority vote was of those who were not in favour of the amendment.[9] The records of the day's debates suggest that there was unrest in the house at the time.[10] Jawaharlal Nehru supported a proposal to postpone the vote, and the vote was postponed accordingly.[11]

This incident proved controversial later on, and objections were raised over the manner in which the vote was shelved. Eventually Karimuddin's amendment was put to vote on a different day with no debate, and was defeated.[12] The consequence was that the privacy principles safeguarding citizens from intrusive search and seizure were never inserted in the Constitution. These principles are a part of what the Supreme Court later recognized as critical rights. However, Constituent Assembly seems to have made its decision with very little meaningful debate on the subject.

The only arguments offered against the insertion of this right, were offered by P.S. Deshmukh in the context of a similar amendment moved by Pandit Thakur Das Bhargva. Bhargva's amendment contained text requiring that "no person shall be subjected to unnecessary restraints or to unreasonable search of person or property", echoing the Karimuddin amendment.[13] Deshmukh was not

---

5 Amendment 512 moved by Kazi Syed Karimuddin, Constituent Assembly Debates, Volume VII, Constituent Assembly Of India (3-12-1948).

6 Amendment 512 moved by Kazi Syed Karimuddin, Constituent Assembly Debates, Volume VII, Constituent Assembly Of India (3-12-1948).

7 Amendment 512 moved by Kazi Syed Karimuddin, Constituent Assembly Debate, Volume VII, Constituent Assembly Of India (3-12-1948).

8 Amendment 512 moved by Kazi Syed Karimuddin, Constituent Assembly Debates, Volume VII, Constituent Assembly Of India (3-12-1948).

9 Constituent Assembly Debates, Volume VII, Constituent Assembly Of India (3-12-1948).

10 Constituent Assembly Debates, Volume VII, Constituent Assembly Of India (3-12-1948).

11 Constituent Assembly Debates, Volume VII, Constituent Assembly Of India (3-12-1948).

12 Constituent Assembly Debates, Volume VII, Part II, Constituent Assembly Of India (6-12-1948).

13 Constituent Assembly Debates, Volume IX, Constituent Assembly Of India (15-9-1949)

convinced of its necessity and he said that the Criminal Procedure Code offered adequate safeguards, but that its provisions were not respected.[14] He argued that it would therefore follow that similar principles inserted in the Constitution would also be ignored.[15] In a speech riddled with inconsistencies, he made the very curious argument that the liberties granted to the people prior to independence would be unsustainable after independence; and that fettering the parliament's discretion with procedure in the context of law and order would be wrong.[16] It is unclear whether this reasoning prevailed, or whether concerns which were not properly articulated during the Constituent Assembly's sessions influenced the vote.

Apart from privacy in the context of search and seizure, the need for the right to privacy in the context of correspondence was also highlighted to the Constituent Assembly. Communication surveillance was addressed in an amendment moved by Somnath Lahiri. This was to include a clause protecting the privacy of correspondence within the fundamental right of liberty (which later became Article 19) in the Constitution.[17] The house resolved to take up the Lahiri proposal towards the end of the discussion on the fundamental rights instead of in the context of the right to liberty. It appears however that the proposal was never seriously considered or even put up for vote.

The records of the Constituent Assembly debates are therefore disappointing if one is seeking powerful reasoning to explain the omission of the right to privacy. There were members who made a powerful case for the inclusion of this right on more than one occasion, but for reasons that are not entirely clear, their arguments were brushed aside.

B. The Supreme Court of India Traces Out Citizens' Rights Against Illegal Surveillance

While the constitution and the choices made about the Fundamental Rights were still fresh in public memory in 1954, the apex court refused to read the right to privacy[18] into the Indian Constitution. This was in *M.P. Sharma* v. *Satish Chandra*, where the Supreme Court declared that it could not import the right to privacy analogous to the U.S. Fourth Amendment into a different fundamental right given that the constitution makers had not thought to recognize this right to privacy.[19]

However, the apex court gradually moved away from this position, to recognizing that other rights and liberties guaranteed in the Constitution would be

[14] Constituent Assembly Debates, Volume IX, CONSTITUENT ASSEMBLY OF INDIA (15-9-1949).
[15] Constituent Assembly Debates, Volume IX, CONSTITUENT ASSEMBLY OF INDIA (15-9-1949).
[16] Constituent Assembly Debates, Volume IX, CONSTITUENT ASSEMBLY OF INDIA (15-9-1949).
[17] Constituent Assembly Debates, Volume III, CONSTITUENT ASSEMBLY OF INDIA (30-4-1947).
[18] *M.P. Sharma* v. *Satish Chandra*, AIR 1954 SC 300.
[19] *M.P. Sharma* v. *Satish Chandra*, AIR 1954 SC 300.

seriously affected if the right to privacy was not protected. This process began in *Kharak Singh* v. *State of U.P.*[20], where the court discussed the relationship between surveillance and personal liberty (personal liberty being guaranteed by the Constitution) and found that unauthorised intrusion into a person's home would interfere with her right to personal liberty. The right to privacy here was conceived around the home, and unauthorised intrusions into homes were seen as interference with the right to personal liberty. The court recognised "*the right of the people to be secure in their persons, houses, papers, and effects*" and declared that their right against unreasonable searches and seizures was not to be violated.[21]

However this right was not seen to extend to the shadowing of citizens outside their homes. In a dissent opinion that exhibited extraordinary foresight, Justice Subba Rao maintained that broad surveillance powers put innocent citizens at risk, and that the right to privacy is an integral part of personal liberty.[22] Subba Rao recognised that when a person is shadowed, her movements will be constricted, and is certainly not free movement. Although he did not use the phrase, in effect, he took into account what is now known as the 'chilling effect' of law.

The right to privacy as defined by the Supreme Court so far, now extends beyond government intrusion into private homes. In *Gobind* v. *State of M.P.*[23] the Supreme Court said that the Constitution makers '*must be deemed to have conferred upon the individual as again the government a sphere where he should be let alone*'. Along with *Kharak Singh*[24], this marks the beginning of the judiciary reading parts of the Karimuddin amendment into the Constitution. The Supreme Court acknowledged in *Gobind case*[25] that the right to privacy is likely to be built through a process of case-by-case development. This case also made it very clear that wherever the fundamental right to privacy is implicated, a law infringing this right must satisfy the compelling state interest test.[26]

What was implicit in the privacy cases after *Kharak Singh*[27] was stated explicitly in *Collector* v. *Canara Bank*[28], where the Supreme Court said quite clearly that the right to privacy '*deals with persons not places*', and reiterated this position more recently in *Directorate of Revenue* v. *Mohd. Nisar Holia*.[29] The doctrine has therefore expanded beyond the *Kharak Singh*[30] majority judgment to the

---

[20] AIR 1963 SC 1295 ("*Kharak Singh*").
[21] *Kharak Singh*, AIR 1963 SC 1295.
[22] *Kharak Singh*, AIR 1963 SC 1295.
[23] (1975) 2 SCC 148 ("*Gobind*").
[24] AIR 1963 SC 1295.
[25] (1975) 2 SCC 148.
[26] *Gobind*, (1975) 2 SCC 148.
[27] AIR 1963 SC 1295.
[28] (2005) 1 SCC 496 : AIR 2005 SC 186 ("*Canara Bank*").
[29] (2008) 2 SCC 370.
[30] AIR 1963 SC 1295.

wider interpretation advocated by Justice Subba Rao in his dissent. *Canara Bank* also made it clear that inroads into the right to privacy for the purpose of surveillance must be for permissible reasons and according to just, fair and reasonable procedure.[31] State action in violation of this procedure is open to a constitutional challenge.

Most specific to communication surveillance are the safeguards resulting from *People's Union for Civil Liberties (PUCL)* v. *Union of India*[32]. In this case, the Indian Supreme Court declared, that "*the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as 'right to privacy'... telephone conversation is an important facet of a man's private life*".[33] The court ruled that telephone tapping would violate Article 21 of the Indian Constitution unless it was permitted by the procedure established by law, and that it would also violate the right to freedom of speech and expression under Article 19 unless it came within the restrictions permitted by Article 19(2).[34] Further, the Supreme Court clarified that even where law clearly defines the situations in which interception may take place, this law must have procedural backing to ensure that the exercise of power is just and reasonable.[35] The lack of adequate procedural safeguards can mean that the substantive law violates Articles 19 and 21 of the Indian Constitution.

After a very promising narrative that recognized the role played by procedural safeguards in protecting citizens' right to privacy, the Supreme Court regrettably accepted Kapil Sibal's argument that it could not impose prior judicial scrutiny in the absence of a statutory provision supporting such scrutiny. Had the court declared the power to intercept communication under the Telegraph Act constitutionally untenable for this reason, this may have resulted in the introduction of powerful safeguards. However the court opted instead to craft interim procedural safeguards for the interception of communication under the Telegraph Act. These safeguards consisted mostly of proper record-keeping and internal executive oversight by senior officers such as the home secretary, the cabinet secretary, the law secretary and the telecommunications secretary.[36] They are opaque and rely solely on members of the executive to review surveillance requests, leaving little for third party scrutiny, or challenge by affected parties (who may never find out that they were placed under surveillance).[37]

This highly inadequate and flawed process was included in the Telegraph Act and the Information Technology Act, as a result of which the Supreme Court of

---

[31] (2005) 1 SCC 496 : AIR 2005 SC 186.
[32] (1997) 1 SCC 301 : AIR 1997 SC 568 ("*PUCL*").
[33] *PUCL*, (1997) 1 SCC 301 : AIR 1997 SC 568.
[34] *PUCL*, (1997) 1 SCC 301 : AIR 1997 SC 568.
[35] *PUCL*, (1997) 1 SCC 301, para 30 : AIR 1997 SC 568.
[36] *PUCL*, (1997) 1 SCC 301 : AIR 1997 SC 568.
[37] *See* also Chinmayi Arun, *Big Brother is watching you*, THE HINDU, (3-1-2014).

India missed a very significant opportunity to raise the minimum standards of privacy protection in the context of surveillance of communication.

II. MASS SURVEILLANCE AND INTERNATIONAL HUMAN RIGHTS NORMS

Our communication interception jurisprudence has focused on targeted surveillance for years. Rapid evolution in technology has however enabled surveillance which is different from targeted surveillance and its identification particular individuals or organizations for monitoring. Mass surveillance operates very differently from targeted surveillance: states have bulk access to communication content and related information, and are able to mine all communication data for specific keywords or other information that might result in the identification of targets.[38]

The international safeguards recommended for targeted surveillance assume some prior suspicion of the target of surveillance. The clarity about the objective and the target makes it easier for 'objective assessment of the necessity and proportionality of the contemplated surveillance, weighing the degree of the proposed intrusion against its anticipated value to a particular investigation'.[39] These safeguards for targeted surveillance emerge from International Human Rights legal norms that require that there must be clear justification whenever there is any interference with the right to privacy, such that there is a proportionality analysis that ensures that there is compelling justification for any serious interference with protected human rights.[40]

The European Court of Human Rights has had occasion to consider this question of mass-surveillance in *Liberty* v. *United Kingdom*[41]. This was a case that resulted after the Ministry of Defence in the United Kingdom operated a powerful facility that simultaneously intercepted a very large number of telephone channels carrying facsimile, email, telephone and data communication. The only safeguards in place were internal, consisting of broad warrants that covered several classes of communication, certification by the Secretary of State of broad classes of information extracted with no discusses of specific targets or

---

[38] Mass surveillance is described as "generalised suspicion" that as yet unidentified members of a group may be of interest, as opposed to personalised surveillance which deals with identified individuals who have triggered suspicion or concern. *See* Roger Clark, *Information Technology and Dataveillance* (November 1987) available at <http://www.rogerclarke.com/DV/CACM88.html#MDV>.

[39] Para 7, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, UNITED NATIONS GENERAL ASSEMBLY (23-9-2014).

[40] Para 12, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, UNITED NATIONS GENERAL ASSEMBLY (23-9-2014).

[41] Application No. 58243 of 2000 (European Court of Human Rights).

addresses, filtering search terms based on the certificates and restriction of sharing the information only with recipients whose purposes to receive them were proportionate and necessary. The court found these safeguards inadequate, particularly since the warrants and certification were framed in very wide terms. It found that the scope or manner of exercise of the state's interception power was not articulated with enough clarity, and there was no publicly accessible and clearly defined procedure followed for the selection, examination, storage, sharing and destruction of intercepted material. Although the court found that the United Kingdom's process contravened the privacy protection offered under the European Convention of Human Rights, it did not clarify the specifics of what might be an acceptable set of safeguards in the context of mass surveillance.

Drawing upon its own past jurisprudence, the European Court insisted on reasonable procedural safeguards. It stated quite clearly that there are significant risks of arbitrariness when executive power is exercised in secret and that law should be sufficiently clear to give citizens an adequate indication of the circumstances in which interception might take place. Additionally, the extent of discretion conferred and the manner of its exercise must be clear enough to protect individuals from arbitrary interference.

This question is likely to be examined in more detail by the court in the near future: London-based organisations Big Brother Watch, Open Rights Group, English PEN and Constanze Kurz have brought the UK government before the ECHR for the mass surveillance of data conducted by British spy agencies.

The United Nations is also veering towards framing useful norms - it has recently passed a resolution[42] calling upon states to review their procedures, practices and legislation with respect to communication surveillance, including mass surveillance, with a view to upholding privacy rights. The UN Special High Commissioner for Human Rights Navi Pillay, in her report titled 'The right to privacy in the digital age' has emphasized the importance of safeguards to protect rights during mass surveillance, and has pointed out that internal procedural safeguards without independent external monitoring are inadequate for the protection of rights.[43] This report declares that effective protection of the law can only be achieved if all the branches of government as well as an independent civilian oversight agency are built into the procedural safeguards.[44] It also lists among these safeguards, that known and accessible remedies are made available to those whose privacy is violated.[45] These remedies must be effective, and must

[42] UN General Assembly, Resolution on Right to Privacy in the Digital Age, 69th session, A/C.3/69/L.26/Rev.1 (19-11-2014).

[43] *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/3, para 37.

[44] *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/3, para 37.

[45] [45] *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/3, para 40.

include a thorough and impartial investigation, the capacity to end ongoing violation and must even offer criminal prosecution as a remedy for gross violations.[46]

III. CONCLUSION: NO EXCUSE FOR INEFFECTIVE SAFEGUARDS

Our safeguards in India apply only to targeted surveillance, and require written requests to be provided and reviewed before telephone tapping or interception is carried out. India has no requirements of transparency whether in the form of disclosing the quantum of interception taking place each year, or in the form of subsequent notification to people whose communication was intercepted. It does not even have external oversight in the form of an independent regulatory body or the judiciary to ensure that no abuse of surveillance systems takes place. Given these structural flaws, the Gujarat illegal surveillance controversy is unsurprising. The complete lack of accountability for the misuse of the surveillance framework in that context bodes ill for the manner in which surveillance is likely to be used in India.

In this context, mass surveillance and the Central Monitoring system (CMS) raises real concerns of extensive misuse of power by the state. News reports in India indicate this is a move towards intercepting all communication over the internet in India and scanning it for keywords like 'attack', 'bomb', 'blast' or 'kill'. Tweets, status updates, emails, chat transcripts, and even voice traffic over the Internet (including from platforms like Skype and Google Talk) will be scanned by this system. In the context of surveillance of phone-calls CMS is even more opaque than targeted surveillance since the state can intercept communication directly, without making requests to private telecommunication service provider. This means that there is one less layer of scrutiny through which abuse of power can reach the public. There is no one to ask whether the requisite paper work is in place or to notice a dramatic increase in interception requests.

Unfettered mass surveillance does not augur well for democracy. Understanding why this is so can be difficult owing to the nature of privacy harms arising from mass surveillance. There are different kinds of privacy harms that may result from surveillance, like disruption of valuable activity, and the chilling of socially beneficial behavior like free speech.[47] Among these is the creation of power imbalances like (excess executive power) that damage the social structure.[48] These different harms tend to be acknowledged in a piecemeal fashion depending on context. For example, in *Kharak Singh*[49], the problem was one

---

[46] *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/3, para 41.

[47] Daniel Solove, *I've Got Nothing to Hide*, 44 San Diego Law Review, 745, 758 (2007).

[48] Daniel Solove, *I've Got Nothing to Hide*, 44 San Diego Law Review, 745, 758 (2007).

[49] AIR 1963 SC 1295.

[50] (1997) 1 SCC 301 : AIR 1997 SC 568.