PUCL V. UNION OF INDIA REVISITED: WHY INDIA'S SURVEILLANCE LAW MUST BE REDESIGNED FOR THE DIGITAL AGE

Chaitanya Ramachandran[*]

The Supreme Court's 1996 judgment in People's Union for Civil Liberties (PUCL) v. Union of India *was a significant attempt to solve the problem of widespread telephone tapping, and its influence has been strongly felt in subsequent laws designed to balance the right to privacy against the state's power to conduct surveillance. The safeguards against arbitrariness in the exercise of the state's surveillance powers designed by the Court continue to apply in the Internet age. However, new mass surveillance programs being undertaken by the Indian government that are unprecedented in their scope necessitate a thorough re-examination of our privacy laws. This note explains how the PUCL guidelines have influenced Indian surveillance law over the past two decades, the manner in which the safeguards designed by the Court have not always worked (or have been circumvented), and argues that with the Internet taking over the telephone as perhaps the most important mode of communication in India today, the time has come to revisit India's surveillance laws to better protect the right to privacy.*

I. INTRODUCTION

In the spring of 1990, Chandra Shekhar (who would soon become the eighth Prime Minister of India) publicly levelled a sensational allegation against the V.P. Singh-led government of the day – that it was illegally tapping the telephones of 27 politicians, including his own.[1] The allegation snowballed into a national scandal, resulting in a Central Bureau of Investigation ('CBI') inquiry that would reveal just how extensive, commonplace, and illegal telephone tapping had become during India's politically turbulent 1980s and early 1990s. The CBI report opened a Pandora's box by detailing the excesses of the Rajiv Gandhi regime of the 1980s, which had surveilled not only its opposition,

[*] Chaitanya Ramachandran is a practicing lawyer specialising in Internet law, based in New Delhi. He holds an LL.M. degree from Stanford Law School and a B.A., LL.B. (Hons.) degree from the National Law School of India University.

[1] India Today, *Scandalous Revelations: Secret Report by CBI contains shocking details of phone tapping ordered by Congress(I) Govts*, February 28, 1991, available at http://indiatoday.intoday.in/story/secret-report-by-cbi-contains-shocking-details-of-phone-tapping-ordered-by-congressi-govts/1/317946.html (Last visited on May 24, 2014).

but even its own Cabinet Ministers and the political leaders of many states.[2] It also exposed the inadequate legal framework and procedural lapses that made such abuses of power possible – tapping was regularly carried out without proper authorisation, persisted for longer periods than was legally permissible, and was often based on specious grounds.[3]

The matter reached the Supreme Court of India through a public interest petition filed by the People's Union for Civil Liberties. Kuldip Singh, J.'s landmark 1996 judgment in *People's Union for Civil Liberties (PUCL)* v. *Union of India*[4] ('PUCL') affirmed that telephone tapping infringed the fundamental right to privacy, and created safeguards against arbitrariness in the exercise of the state's surveillance powers.

Yet, even though the Court crafted the PUCL guidelines as a temporary solution pending remedial action by the central government against the misuse of its surveillance powers,[5] the guidelines cast a long shadow over Indian surveillance law. Their influence continues to be felt in the age of the Internet, as recent laws governing Internet surveillance derive much inspiration from the PUCL doctrine.[6] In this note, I critically re-examine the PUCL decision against the backdrop of pervasive Internet surveillance in the India of 2014. While I acknowledge that the decision was an important attempt to solve a pressing problem, I argue that the heightened risks presented by surveillance today necessitate a far more comprehensive restructuring of surveillance law in India. I first summarise the PUCL decision and demonstrate how the safeguards devised by the Court cast a long shadow over subsequent laws relating to surveillance. I then argue that recent state surveillance projects demonstrate that these safeguards can no longer act as a check on arbitrariness, and finally make the case for a substantial redesign of India's surveillance laws.

II. THE PUCL DECISION AND ITS CONTINUING INFLUENCE

PUCL was a landmark decision for two reasons. *First*, the Court reflected, at some length, upon the existence of a right to privacy in Indian law. Specifically, it considered the question of whether the right to privacy was a fundamental right guaranteed by the Constitution. This was important to the outcome of the case for, if telephone tapping infringed a fundamental right, it would have to satisfy a stricter level of judicial review. *Second*, the Court laid down detailed guidelines for the exercise of the executive's surveillance

2 *Id*.
3 *Id*.
4 People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
5 *Id*., ¶46.
6 *See* discussion *infra* Part II C.

powers, as a temporary solution to the rampant misuse of these powers that had precipitated the case.

A. THE RIGHT TO PRIVACY

On the question of the existence of a right to privacy, the Court first cited its 1962 decision in *Kharak Singh* v. *State of U.P.*[7] ('Kharak Singh'), in which it had considered the effect of police surveillance (in the form of 'domiciliary visits' involving local police constables entering the petitioner's house at night) on the petitioner's right to privacy. The Kharak Singh Court recognised a 'right to privacy' in Indian law, albeit not one guaranteed by the Constitution.[8] The PUCL Court also cited with approval Subba Rao, J.'s minority opinion in Kharak Singh, which expanded the scope of the right granted by Article 21 to include the "right of an individual to be free from restrictions or encroachments on his person".[9]

---

7 Kharak Singh v. STATE OF U.P., AIR 1963 SC 1295.

8 *Id*., ¶15 ("[A]n 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, if not of the very concept of civilisation. An English Common Law maxim asserts that 'every man's house is his castle' and in Semayne's case, where this was applied, it was stated that 'the house of everyone is to him as his castle and fortress as well as for his defence against injury and violence as for his repose'. We are not unmindful of the fact that Semayne's case was concerned with the law relating to executions in England, but the passage extracted has a validity quite apart from the context of the particular decision. It embodies an abiding principle which transcends mere protection of property rights and expounds a concept of 'personal liberty' which does not rest on any element of feudalism or on any theory of freedom which has ceased to be of value.").

With respect to those clauses of the impugned U.P. Police Regulations that related to shadowing, reporting of movements, and verification of such movements through enquiries, of 'history-sheeters', the majority in Kharak Singh found that these implicated a privacy interest and held 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 (¶17). Instead, the majority only struck down the clause of the Regulations that authorised 'domiciliary visits' for the purpose of surveillance as being violative of the right to life and personal liberty under Art. 21 (¶28). By contrast, Subba Rao, J.'s forward-looking minority opinion went much further by finding the entire impugned Regulation (and not just the clause dealing with domiciliary visits) unconstitutional, on the ground (among others) that although "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" – a far more expansive view of Art. 21, foreshadowing by many years the radical re-imagining of the scope of that Article in *Maneka* Gandhi v. Union of India, (1978) 1 SCC 248.

9 Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332, ¶38 ("If physical restraints on a person's movements affect his personal liberty, physical encroachments on his private life would affect it in a larger degree. Indeed, nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy. We would, therefore, define the right of personal liberty in Art. 21 as a right of an individual 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.").

Another case cited by the PUCL Court, *Gobind* v. *State of M.P.*,[10] which, like Kharak Singh,[11] dealt with real-world police surveillance, established the need for laws infringing privacy claims to satisfy a heightened standard of judicial review – the "compelling State interest" test.[12] The Court was not yet ready to elevate the right to privacy as a fundamental right.[13]

The PUCL Court also relied on its 1994 decision in *R. Rajagopal* v. *State of Tamil Nadu* ('Rajagopal'),[14] a case that elevated the right to privacy to Constitutional status by virtue of it being "implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21"[15] – a right that may not be violated except "according to procedure established by law".[16] The Court in that case also expanded the notion of the right to privacy to include a right "to be let alone", and to "safeguard the privacy of [a person], his family, marriage, procreation, motherhood, child-bearing and education among other matters".[17]

The above cases, from Kharak Singh to PUCL, show the evolution of the Supreme Court's conception of privacy. The Kharak Singh Court referred to the physical privacy of the person – the right to "be free from restrictions or encroachments on his person".[18] This notion was expanded in Rajagopal, a case which concerned the publication of the autobiography of the serial killer Auto Shankar; the autobiography implicated senior police officials in acts of corruption and collusion. As the privacy right at issue here was that of the reputation of police officials, its recognition by the Court expanded the right to privacy beyond the physical realm. The PUCL Court further evolved the notion of privacy to include personal communications, holding 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'".[19] To the

[10] Gobind v. State of M.P., (1975) 2 SCC 148.

[11] AIR 1963 SC 1295.

[12] Kharak Singh, *supra* note 7, ¶22 ("There can be no doubt that privacy dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling State interest test. Then the question would be whether a State interest is of such paramount importance as would justify an infringement of the right. Obviously, if the enforcement of morality were held to be a compelling as well as a permissible State interest, the characterisation of the claimed rights as a fundamental privacy right would be of far less significance.").

[13] Kharak Singh, *supra* note 7, ¶28 and ¶30 ("Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterise as a fundamental right, we do not think that the right is absolute."; "[W]e are satisfied that drastic inroads directly into the privacy and indirectly into the fundamental rights, of a citizen will be made if Regulations 855 and 856 were to be read widely.").

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

[15] *Id*., ¶28.

[16] The Constitution of India, 1950, Art. 21.

[17] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632, ¶26.

[18] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295, ¶28: (1964) 1 SCR 332. ¶38.

[19] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, ¶18.

contemporary reader, it might seem natural for this evolving understanding of privacy to now encompass online communications.

B. GUIDING THE EXERCISE OF THE STATE'S SURVEILLANCE POWERS

The question at the heart of the PUCL decision was the validity of §5(2)[20] of the Indian Telegraph Act, 1885,[21] which the Court declined to strike down as unconstitutional. Instead, it stressed at length the need for the executive to adhere to the two statutory pre-conditions for the exercise of the power to intercept (either the "occurrence of any public emergency" or "the interest of public safety") and the five permitted grounds for the issuance of an interception order.[22]

The PUCL Court also laid down detailed safeguards designed to check arbitrariness in the issuance of telephone tapping orders, including the following measures:[23]

1. Orders for telephone tapping may only be issued by the Home Secretary of the central government or a state government. In an emergency, this power may be delegated to an officer of the Home Department of the

[20] Indian Telegraph Act, 1885, §5(2) ("Power for Government to take possession of licensed telegraphs and to order interception of messages – […] (2) On such occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government 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 an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought by transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:

Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.").

[21] *See generally* J.H. Lienhard, *Indian Telegraph*, available at http://www.uh.edu/engines/epi1380.htm (Last visited on December 1, 2014) (The Indian Telegraph Act, 1885 is a British Raj era law still in force today. Its initial purpose was to cement the Crown's authority over telegraphs in India, which had become indispensable to the colonial administration; indeed, the completion of the trans-India telegraph was instrumental to its ability to put down the Revolt of 1857. "One captured rebel, being led to the gallows, pointed to a telegraph line and bravely cried, 'There is the accursed string that strangles us.'" The Act, therefore, was – in a sense – designed to help the Government of the day quell dissent.).

[22] The five permitted grounds for the issuance of an interception order under Indian Telegraph Act, 1885, §5(2) are: (i) Sovereignty and integrity of India; (ii) security of the State; (iii) friendly relations with foreign States; (iv) public order; (v) preventing incitement to the commission of an offence.

[23] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, ¶35.

central or state government, and a copy of the order must be sent to the concerned Review Committee (see below) within one week.

2. The authority making the order must consider whether the information which is considered necessary to acquire could reasonably be acquired by other means.

3. Orders issued under the Indian Telegraph Act, 1885 shall be valid for two months from the date of issue.

4. Review Committees shall be constituted consisting of Secretary-level officers at both the central and state levels. They may evaluate whether an interception order has been passed in compliance with the law, and if it has not, they may set it aside and direct the destruction of any copies of the intercepted communications.

5. The authority issuing the interception order must maintain records of: (i) the intercepted communications; (ii) the extent to which material is disclosed; (iii) the number of persons to whom the material is disclosed and their identity; (iv) the extent to which the material is copied; and (v) the number of copies made (each of which must be destroyed as soon as its retention is no longer necessary).

The PUCL Court notably declined to impose the procedural safeguard of prior judicial scrutiny (such as by the issuance of a warrant) for interception orders, which the petitioners had argued would be the only way to safeguard the right to privacy of an individual, as "judicial scrutiny alone would take away the apprehension of arbitrariness or unreasonableness […]".[24] The Court's stated reason was that it could not require prior judicial scrutiny in the absence of a provision to that effect in the statute.[25] By contrast, the Code of Criminal Procedure, 1973, ('CrPC') does provide for the issuance of a search warrant by a court to compel the production of a "document or other thing".[26] However, even under the CrPC, information may be obtained without a warrant if an officer in charge of a police station issues a written order to the person in possession of the information sought.[27]

[24] *Id*., ¶33.
[25] *Id*.
[26] Code of Criminal Procedure, 1973, §93(1).
[27] *Id*., §91.

C. THE CONTINUING INFLUENCE OF THE PUCL GUIDELINES

The PUCL guidelines were eventually codified (in a somewhat modified form) by Rule 419-A of the Indian Telegraph Rules, 1951. Some of the key embellishments introduced by Rule 419-A are as follows:

1. The emergency powers are expanded to include interception at the direction of senior law enforcement officers in emergent cases, either in remote areas or for operational reasons, in either case where it is not feasible to obtain prior directions. Orders issued under such circumstances must be communicated to the competent authority within three working days, and confirmed within seven working days.[28]

2. The total period of interception (including renewals of the interception order) is limited to 180 days.[29]

3. Telecommunications service providers are required to designate two senior executives as nodal officers to receive and handle interception orders. They must acknowledge receipt of the interception order within two hours, and submit a list of all interception orders received to the nodal officers of the requisitioning security and law enforcement agencies for verification.[30]

4. The Review Committees at the central and state levels must meet at least once in two months and record their findings on whether the interception directions issued conform to §5(2) of the India Telegraph Act, 1885.[31]

The influence of the PUCL guidelines extends beyond the realm of telecommunications surveillance; the regime for the interception of digital communications created by the Information Technology Act, 2000 ('IT Act'), is heavily influenced by them. The IT Act, a broad-ranging legislation regulating various aspects of information technology in India, deals with digital surveillance and grants wide powers to the central and state governments to order the interception, monitoring, or decryption of "any information generated, transmitted, received or stored in any computer resource",[32] which potentially covers most forms of digital communication. The grounds on which these powers may be exercised are slightly broader than those under the Indian Telegraph Act,

[28] Indian Telegraph Rules, 1951, Rule 419-A(1).
[29] *Id*., Rule 419-A(6).
[30] *Id*., Rules 419-A(10), (11), and (12).
[31] *Id*., Rule 419-A(17).
[32] Information Technology Act, 2000, §69(1).

1885.[33] However, the most significant difference is that the two preconditions for the exercise of the surveillance powers under the Indian Telegraph Act, 1885, (namely the "occurrence of any public emergency" or "the interest of public safety") are absent from the IT Act, and so there is no threshold test that must be satisfied before the powers under the latter Act are exercised. The procedure and safeguards relating to these powers are specified in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, and are very similar to Rule 419-A – therefore continuing PUCL's lineage.

III. THE RISE OF 'BIG BROTHER' IN INDIA AND THE FAILURE OF SAFEGUARDS AGAINST ARBITRARINESS

Although illegal telephone-tapping at the dawn of the 1990s was rampant enough to create a national outcry, it would probably pale in comparison to the state's surveillance projects in 2014. Today, interest in surveillance has been piqued by two important developments. *First*, the surveillance disclosures triggered by Edward Snowden in 2013,[34] which were responsible for exposing the astonishing scope of surveillance activities carried out by the government of the United States of America (of which India was a prominent target);[35] *second*, regular (albeit piecemeal) revelations of the Indian government's ongoing efforts to implement massive surveillance projects to monitor communications data on a national scale. These projects have placed India at par with the USA and UK with respect to online surveillance,[36] and signal the beginning of mass surveillance in India, as compared to the targeted surveillance that PUCL sought to remedy. Some of the prominent surveillance projects currently being undertaken by the Indian government include:

The Central Monitoring System ('CMS'): The CMS is a system developed by the Centre for Development of Telematics (C-DoT) that grants direct, centralised access to communications data (including mobile and landline

---

[33] The grounds on which the powers granted by the Information Technology Act, 2000, §69(1) may be exercised are: (i) the sovereignty or integrity of India; (ii) defence of India; (iii) security of the State; (iv) friendly relations with foreign States; (v) public order; (vi) for preventing incitement to the commission of any cognizable offence; and (vii) for investigation of any offence.

[34] The Guardian, *The NSA Files*, available at http://www.theguardian.com/us-news/the-nsa-files (Last visited on December 1, 2014).

[35] The Hindu, *India Among Top Targets of Spying by NSA*, September 23, 2013, available at http://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece (Last visited on May 25, 2014).

[36] India Today, *Forget NSA, India's Centre for Development of Telematics is One of Top 3 Worst Online Spies*, March 12, 2014, available at http://indiatoday.intoday.in/story/indias-centre-for-development-of-telematics-worst-online-spies-reporters-without-borders/1/347920.html (Last visited on May 25, 2014).

calls, Voice over IP ('VoIP') calls, emails, and Internet communication including on social media) to authorised security agencies. It augments the existing 'lawful interception and monitoring systems' ('LIM') that telecommunications service providers are already required to install by additionally requiring them to integrate 'interception, store and forward' servers with the LIM systems. These are connected to regional monitoring centres of the CMS, which are in turn connected to the CMS itself.[37] This implies that the CMS will have centralised and real-time access to virtually all communications data (both content and metadata), and also that security agencies will be able to bypass telecommunications service providers and directly access such data. Telecom service providers will be obliged to co-operate with the government in setting up the CMS, as this has been incorporated into their operating licenses.[38] There is very little publicly available information about the CMS and its current operational status.

National Intelligence Grid ('NATGRID'): NATGRID was proposed in the aftermath of the 26/11 terrorist attack. It is an initiative of the Union Home Ministry to integrate the data sources of various intelligence and law enforcement agencies in order to identify intelligence-related patterns that can be accessed by intelligence agencies.[39] The types of data that are gathered in the NATGRID database include tax and bank account details, credit card transactions, visa and immigration records and air and rail travel itineraries.[40]

Network Traffic Analysis ('NETRA'): NETRA is a tool developed by the Centre for Artificial Intelligence and Robotics (CAIR) of the Defence Research and Development Organisation ('DRDO') to analyse Internet traffic based on pre-defined filters.[41] Data types that are expected to be monitored by NETRA include social media platforms (such as Facebook and Twitter), emails, blogs, instant messaging, and VoIP calls (such as Skype and Google Talk), among others.[42] It is unclear how the data to be analysed will be captured by the system, or whether this will be achieved through integration with the CMS.

---

37 Maria Xynou, *India's Central Monitoring System (CMS): Something to Worry About?*, January 30, 2014, available at http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about (Last visited on May 25, 2014).

38 *Id*.

39 The Economic Times, *National Intelligence Grid begins operations; high security protocols deployed*, December 22, 2013, available at http://articles.economictimes.indiatimes.com/2013-12-22/news/45475848_1_natgrid-national-intelligence-grid-raman (Last visited on May 31, 2014).

40 Wikipedia, *NATGRID*, available at http://en.wikipedia.org/wiki/NATGRID (Last visited on December 1, 2014).

41 Times of India, *Govt. to Launch Internet Spy System "Netra" soon*, January 6, 2014, available at http://timesofindia.indiatimes.com/tech/tech-news/Govt-to-launch-internet-spy-system-Netra-soon/articleshow/28456222.cms (Last visited on May 31, 2014).

42 *Id*.; *See also* Diwanshu Wadhwani, *Netra – You Will Be Under Surveillance by Indian Internet Spy System*, January 8, 2014, available at http://newtecharticles.com/netra-indian-government-internet-spy-system/ (Last visited on May 31, 2014).

While it is clear that the Indian government is presently deploying a number of mass surveillance projects, details of their operation, along with the legal safeguards in place to protect the privacy rights of individuals, remain unclear. This lack of information presents a more significant concern than the existence of the surveillance projects. As interpersonal communication is increasingly conducted digitally, it is inevitable that the state's intelligence activities are also increasingly focusing on the digital realm. What is worrying is the government's zeal in commencing these projects without specific statutory backing or oversight (whether by Parliament or the judiciary).

This is worrisome because even prior to the CMS being deployed, existing legal safeguards have not been properly followed. The government is alleged to have direct access to LIM equipment (which, in the case of an Internet Service Provider, is installed between its Internet edge router and its core network), which would permit it to bypass existing legal safeguards including the requirement of an interception order issued to the service provider by the competent authority.[43] Other legal safeguards – such as acknowledgment of receipt of an interception order by the service provider's nodal officers[44] and the verification of interception orders every fifteen days between the service provider and the law enforcement agency[45] – can easily be violated by law enforcement agencies without the service providers having any opportunity to identify the procedural defect.[46] Another transgression is that while the law requires interception orders to be tied to specific addresses,[47] computer resources,[48] or premises[49] identified in the interception order, in practice, security agencies can conduct extremely broad searches using only keywords, which expand the scope of the search far beyond addresses, specific computer resources or premises.[50]

---

[43] The Hindu, *Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic*, September 9, 2013, available at http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece (Last visited on May 31, 2014) ("Since the Government controls the LIMs, it directly sends software commands and sucks out whatever information it needs from the Internet pipe without any intimation or information to anyone, except to those within the Government who send the Internet traffic monitoring commands. No ISP confirmed as to whether they had ever received an "authorisation" letter for interception or monitoring of internet content.").

[44] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 15.

[45] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 18.

[46] The Hindu, *Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic*, September 9, 2013, available at http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece (Last visited on May 31, 2014).

[47] Indian Telegraph Rules, 1951, Rule 419-A(4).

[48] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 9.

[49] Indian Telegraph Rules, 1951, Rule 419-A(4); Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 9.

[50] *Id*.

Another cause for concern is the continued revelation to the public of personal data being obtained by way of unauthorised surveillance. In 2012, a change of government in Himachal Pradesh revealed that the previous regime had targeted 1371 telephone numbers for tapping and recording, but the State's Home Secretary had granted permission for only about 2 per cent of these.[51] In another high-profile case, Call Data Records ('CDRs') of telephone numbers belonging to senior opposition leader Arun Jaitley were obtained in an unauthorised manner – while the opposition argued that the telephone numbers had been tapped,[52] the police claimed that only CDRs had been obtained, and this was done by junior police personnel and private detectives who used a senior police official's e-mail ID without authorisation.[53]

These major lapses – the lack of statutory authorisation for the new surveillance projects, the failure to comply with existing legal safeguards, and continuing revelations of unauthorised surveillance – undermine the government's position on its surveillance activities. In response to a question in the Rajya Sabha in 2013, Milind Deora (then Minister of State for Communications and Information Technology) told Parliament that interception and monitoring under the CMS would only be carried out in compliance with §5(2) of the Indian Telegraph Act, Rule 419-A, and the PUCL guidelines.[54] He also said that the CMS has an in-built system of checks and balances, in that:

> "Law Enforcement Agencies ('LEAs') are not able to provision the target themselves and the provisioning authority is not able to see the content of the intercepted communication. Additionally, there is a provision of auto generation of audit trail of command logs related to interception and monitoring, which works as a deterrent to any unauthorised provisioning."[55]

---

[51] Pranesh Prakash, *Misuse of Surveillance Powers in India (Case 1)*, December 6, 2013, available at http://cis-india.org/internet-governance/blog/misuse-surveillance-powers-india-case1 (Last visited on May 31, 2014).

[52] The Hindu, *Jaitley's Phone Not Tapped but Call Records Accessed*, *Says Shinde*, March 2, 2013, available at http://www.thehindu.com/news/national/jaitleys-phone-not-tapped-but-call-records-accessed-says-shinde/article4465326.ece?ref=relatedNews (Last visited on May 31, 2014).

[53] The Hindu, *Arun Jaitley Phone-Tapping Case: 6 More Held*, November 14, 2013, available at http://www.thehindu.com/news/national/arun-jaitley-phonetapping-case-6-more-held/article5350492.ece (Last visited on May 31, 2014).

[54] Rajya Sabha Debates, *Central Monitoring System Project*, Session Number 229, August 23, 2013, *comments by* Milind Deora, available at http://rsdebate.nic.in/bitstream/123456789/624987/2/PQ_229_23082013_U1598_p165_p166.pdf#search=milind deora (Last visited on May 31, 2014).

[55] *Id*.

The government has also argued that the CMS merely automates existing surveillance procedures.[56] The government's position is unsatisfactory for a number of reasons. *First*, when existing law requires an interface between the authority issuing the interception order and the service providers (for example, the service provider must acknowledge receipt of an interception order),[57] the disintermediation of the service providers (which is the effect of the direct access afforded to security agencies under the CMS) is itself in violation of the law, and not, as the government has claimed, in the service of citizens' privacy because telecommunications companies would no longer be directly involved in the surveillance.[58] *Second*, it is unclear why, when the CMS clearly includes the collection of data transmitted over the Internet such as emails and VoIP calls, the government is citing the Indian Telegraph Act and Telegraph Rules as its legal authority to the exclusion of the IT Act and the IT Rules, which would apply to IP-based communication. *Third*, when existing legal safeguards are routinely being violated under the LIM-based surveillance regime, the argument that they will act as an effective check on the misuse of the CMS rings hollow. A more reasonable conclusion is that the safeguards are inadequate. *Fourth*, it is worrying that a massive project such as the CMS is being executed without any specific statutory backing, and without being overseen either by Parliament or the judiciary. This also exposes a major flaw in existing surveillance law, which currently does not provide for such oversight.[59]

Finally, the widening of the surveillance net to cover a substantial portion of the Indian population harms the prospect of public exposure of governmental overreach in the future. As the examples I have cited above show, illegal surveillance in India tends to come into the public eye only when senior political figures are targeted. The government's mass surveillance projects are capable of targeting anyone who uses telephone or electronic communications in India. Unlike high-profile political figures, the unauthorised surveillance of ordinary citizens is less likely to make headlines, and regular citizens will not have the same ability to protest unauthorised surveillance, whether by publicising it or taking legal action.

---

[56] Press Release, Press Information Bureau, March 9, 2011, available at http://pib.nic.in/newsite/erelease.aspx?relid=70747 (Last visited on May 31, 2014).

[57] For example, Rule 419-A(11) of the Indian Telegraph Rules, 1951 and Rule 15 of the Information Technology Rules, 2009, require the service provider to acknowledge receipt of an interception order. Rule 419-A(13) and Rule 18 of the Information Technology Rules, 2009 require the service providers and security agencies to meet every fifteen days to verify the list of interception orders received. With direct access enabled by CMS, these provisions will become redundant.

[58] Abhi Manyu, Gizmodo, *Milind Deora Actually Believes That CMS Will Protect Your Privacy*, June 8, 2013, available at http://www.gizmodo.in/news/Milind-Deora-Actually-Believes-That-CMS-Will-Protect-Your-Privacy/articleshow/20530388.cms (Last visited on May 31, 2014).

[59] Even the Review Committees required under existing law are located within the executive branch.

IV. THE CASE FOR REDESIGNING INDIA'S SURVEILLANCE LAW

The ease with which existing safeguards for citizens' privacy can be circumvented or violated by new mass surveillance technologies occasions a re-evaluation of India's surveillance laws. The PUCL Court observed that telephone conversations were an important part of modern life, and were "often of an intimate and confidential character".[60] Speaking at the dawn of the mobile telephony revolution in India, the Court observed (somewhat quaintly from today's point of view) that "more and more people are carrying mobile telephone instruments in their pockets".[61] If the PUCL Court were to speak today, it would certainly find contemporary forms of communication (including e-mail, social media, VoIP, and Google searches, among others) to be equally deserving of the Constitution's guarantees of privacy and freedom of expression. If these rights are to be adequately protected, the time has come for another restructuring of India's surveillance laws.

A major defect of the government's mass surveillance projects, including the CMS, is that they exist despite there being no specific statute enabling them. This is a troublesome issue for a very fundamental reason – existing Indian law assumes that surveillance will be targeted. In PUCL , the Court defined 'interception' under §5(2) of the Indian Telegraph Act, 1885 as being the interception of communications sent to or from a specific address, and relating to a specific person, both of which must be specified in the interception order.[62] This concept is echoed by Rule 419-A[63] as well as the IT Act regime.[64] However, the type of surveillance to be carried out using the CMS turns this concept on its head – virtually all communications on the telephone and IP networks in India can be monitored in a blanket fashion (for example, by the use of keywords).[65] As existing law does not contemplate this type of mass surveillance, it is currently being carried out in a legal vacuum with no safeguards for citizens' privacy rights. This is clear governmental overreach.

If the surveillance programmes are to continue, they must be authorised by specific Acts of Parliament that provide more robust safeguards than existing law does. These safeguards must, in their design, be informed by the fundamentally different nature of mass surveillance. They must include, for example, strict time limits on data retention, liability for unauthorised access

60 People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, ¶18.

61 *Id*.

62 *Id*., ¶35.

63 Indian Telegraph Rules, 1951, Rule 419-A(4).

64 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 9.

65 The Hindu, *Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic*, September 9, 2013, available at http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece (Last visited on May 31, 2014).

to, or disclosure of, intercepted communications, and a distinction between the interception of metadata and content (with access to the latter having to pass muster under a stricter standard). These safeguards must be in addition to strengthened versions of existing safeguards regarding when an interception order may be issued, who may issue it, and the information that it must mandatorily contain.

Another major problem with the existing surveillance law regime is its concentration of power within the executive branch of government. The PUCL Court declined to impose the requirement of prior, case-by-case judicial scrutiny for interception requests, and instead left this important gatekeeping function to the executive. This approach needs to be revisited for at least two reasons. *First*, it contravenes the principle of separation of powers, and creates a conflict of interest within the executive branch, which is responsible for both the surveillance of a target individual, and deciding whether the interception of that individual communication would be a reasonable restriction of his right to privacy. With the fundamental rights of hundreds of millions of citizens potentially at risk, which was arguably not the case when PUCL was decided, it is more important than ever that interception requests be individually evaluated to determine whether or not they are legitimate enough to justify infringing an individual's right to privacy.

Second, the experience over the last eighteen years has shown that the PUCL guidelines are prone to being violated without any meaningful consequence for the violator – they just have not worked as well as they were supposed to. This experience leads to the conclusion that bringing the judiciary's expertise to bear in independently testing interception requests against the right to privacy may be the best method of protecting that right. This judicial function could be guided by a "probable cause"-type standard to determine whether or not a warrant should be granted in a given case.[66] The warrant procedure should be specified in an Act of Parliament that enables the government's mass surveillance programs. The procedure need not be public, in order to preserve its confidentiality. But the Act should require that strict records of all warrant proceedings be retained, so that any illegalities can be subsequently detected and remedied. Perhaps most importantly, the warrant process should actually involve case-by-case determination, and should not be a 'rubber stamp'. The

[66] *See* Wex Legal Dictionary, *Probable Cause*, available at http://www.law.cornell.edu/wex/probable_cause (Last visited on December 1, 2014) ('Probable cause' is a concept from American criminal jurisprudence that refers to the standard that must be met by law enforcement agencies in order to receive a warrant. It is useful to note that, "Courts usually find probable cause when there is a reasonable basis for believing that a crime may have been committed (for an arrest), or when evidence of the crime is present in the place to be searched (for a search). Under exigent circumstances, probable cause can also justify a warrantless search or seizure. Persons arrested without a warrant are required to be brought before a competent authority shortly after the arrest for a prompt judicial determination of probable cause.").

supervisory role of the appellate courts will be especially important in enforcing this principle.

V. CONCLUSION

While PUCL will undoubtedly remain a landmark decision in Indian privacy law, it is nevertheless imperative that the law keeps pace with rapidly changing times. Surveillance today is far more pervasive and capable of violating the privacy of the public *en masse* than it was eighteen years ago. Experience has shown that the PUCL guidelines have not been as effective as they were intended to be. The deployment of the largest surveillance programs in Indian history necessitates a fundamental reimagining of Indian surveillance law if the Constitutional right to privacy is to be saved from inconsequence. Systemic Parliamentary sanction of (and oversight over) the government's surveillance projects is imperative. Finally, perhaps the idea of surveillance being based on judicial warrants is an idea whose time in India has finally come.