THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 6, 2010

BALANCING ONLINE PRIVACY IN INDIA

Apar Gupta[*]

ABSTRACT

There have been disturbing press reports and articles on the Information Technology (Amendment) Act, 2008. These accounts broadly wallow about the increase in the police powers of the state. They contend that the amendment grants legal sanction to online surveillance inexorably whittling down internet privacy. This article seeks to examine this prevalent notion. It discovers that legal provisions for online surveillance, monitoring and identification of data have been inserted in a narrow and defined class of circumstances governed by tenuous procedures. At first glance it may seem that these procedures and safeguards by themselves increase the right to privacy. However, on a deeper study it is revealed that they are found wanting due to the nature of internet communications. The article takes a comprehensive look at the state of online privacy in India arising out of the Information Technology Act, 2000.

TABLE OF CONTENTS

[*] Lawyer; LL.M., Columbia Law School, Columbia University in the City of New York.

I

INTRODUCTION

With the decision in *Naz Foundation v. Government of N.C.T.*,[1] there is a growing feeling that privacy rights of individuals are gaining recognition in the Indian legal landscape.[2] What is interesting about the High Court decision reading down section 377 of the Indian Penal Code[3] and decriminalizing homosexual activity[4] is the hesitation of the Union Government to appeal against the verdict in the Supreme Court.[5] Till date, the Union Government remains absent from the list of the 14 appellants[6] appealing the decision.[7] Here it seems counterintuitive that a government which is ostensibly hesitant to challenge a court decision expanding liberal notions of

---

[1] Naz Foundation v. Government of N.C.T. of Delhi & Ors., 160 (2009) D.L.T. 277 (India) (*Per* A. P. Shah, C.J. & S. Muralidhar, J.). It concerned a constitutional challenge to section 377 of the Indian Penal Code, 1860 which criminalised unnatural consensual sexual acts between adults. The petitioner claimed and secured a limited relief amounting to limiting the application of the section to non-consensual penile non-vaginal sex and penile non-vaginal sex involving minors only.

[2] Lawrence Liang, Is the Naz Foundation decision the Roe v. Wade of India? (Kafila Blog, July 6, 2009), http://kafila.org/2009/07/06/is-the-naz-foundation-decision-the-roe-v-wade-of-india/ (last visited Dec. 25, 2009); *see also* Leonard Link, Indian Court Rules on Colonial-Era Sodomy Law (Leonard Link's Blog, July 2, 2009), http://newyorklawschool.typepad.com/leonardlink/2009/07/indian-court-rules-on-colonialera-sodomy-law.html (last visited Dec. 25, 2009).

[3] INDIA PEN. CODE, 1860, No. 45 of 1860.

[4] *Supra* note 1, at ¶ 132.

[5] *Govt unlikely to appeal HC's Gay Order on its own*, TIMES OF INDIA, July 3, 2009, *available at* http://timesofindia.indiatimes.com/india/Govt-unlikely-to-appeal-HCs-gay-order-on-its-own/articleshow/4730486.cms.

[6] Case Status – Supreme Court of India, http://courtnic.nic.in/courtnicsc.asp (search in 'Title' + 'Respondent' + '2009' & '2010,' on the string 'Naz Foundation') (last visited July 4, 2010).

[7] Suresh Kumar Koushal v. Naz Foundation, SLP(C) No. 15436/2009 (last order dated July 20, 2009), *available at* http://courtnic.nic.in/supremecourt/temp/dc%201543609p.txt; *see* Arvind Gopal, Suresh Kumar Koushal v. Naz Foundation SLP(C) No. 15436/2009 (Lawyers Collective HIV/AIDS Unit – s377 Case Updates, July 22, 2009), http://www.lawyerscollective.org/node/1022.

individual rights would pass a law greatly curtailing online privacy.[8] Hence, a casual reading of the recently introduced sections 69 and 69B of the Information Technology Act, 2000[9] would take an observer by surprise. Comparatively viewed, the absence of a challenge to the *Naz Foundation* decision will seem less than an accident and nothing more than serendipity.

The provisions which have been introduced by a recent amendment have vested state functionaries with the powers to intercept, monitor and decrypt information,[10] block access to websites[11] and monitor or collect traffic data.[12] Prior to this amendment, there was a vacuum in Indian law[13] where interception and monitoring in relation to internet communications was being carried out under the general provisions of the Indian Telegraph Act, 1885.[14] The recent amendment did not go unnoticed with one commentator noting that the provisions are "far more intrusive than the Indian Telegraph Act of 1885, which was drafted to protect the interests of the British Raj."[15] Others chimed in with Orwellian brooding.[16] Though a well articulated defence of such a position was found lacking, the principal contention advanced was premised on the claim that the provisions for intrusion, *ipso jure* constituted a breach of the right to online privacy.

This article does not merely proceed on the premise that the very existence of the legal sanction results in a breach of privacy. This article is geared towards a realist conception of privacy rights

---

[8] *See* Rukmini Sen, *Breaking Silences, Celebrating New Spaces: Mapping Elite Responses To The 'Inclusive' Judgment*, 2 NUJS L. REV. 480, 490 (2009) ("[i]t is a judgment which causes for celebration as has expectedly happened, but it also raises doubts on whether this can be sustained, and the legislature will start from where the judiciary ended rather than reinventing.").

[9] Information Technology (Amendment) Act, 2008, No. 10 of 2009.

[10] § 69, Information Technology (Amendment) Act, 2008, No. 10 of 2009.

[11] § 69A, Information Technology (Amendment) Act, 2008, No. 10 of 2009. Even though this section does affect the civil liberties of an individual, it is outside the scope of the present article, as the right being analysed in this article is the right to privacy and not the right to speech and expression.

[12] § 69B, Information Technology (Amendment) Act, 2008, No. 10 of 2009.

[13] Siddharth Srivastava, *Email Users Beware, Big Brother is Watching*, TIMES OF INDIA, Dec. 24, 2001, *available at* http://timesofindia.indiatimes.com/articleshow.asp?art_id=37906058. It observes that the intelligence bureau has prepared a list of new keywords in 2001 to intercept mails emanating from IP addresses in India suggesting that interception was occurring despite the presence of any specific law.

[14] Indian Telegraph Act, 1885, No. 13 of 1885 (hereinafter 'Telegraph Act').

[15] Kounteya Sinha & Mahendra Kumar Singh, *New law will let Govt Snoop on your PC*, TIMES OF INDIA, Dec. 25, 2008, *available at* http://timesofindia.indiatimes.com/India/New_law_will_let_govt_snoop_on_your_PC/articleshow/3888633.cms.

[16] *Yes, Snooping's Allowed*, INDIAN EXPRESS, Feb. 6, 2009, *available at* http://www.indianexpress.com/news/yes-snoopings-allowed/419978/ ("[u] nder the new IT Act, any Government official or policeman will be able to listen to all your phone calls, read your SMSs and emails, and monitor the websites you visit. And he will not require any warrant from a magistrate to do so.").

and does not posit them in an overly broad or moralistic hue. It does not quibble over the definition or the underlying jurisprudence of the right but however, proceeds to analyse the likely harms which may be caused due to a breach.[17] It also studies the protections which have been made against gathering and dissemination of information, towards the broader goal of reviewing internet privacy laws in India.[18] To this purpose, Part II utilizes two popular taxonomies adopted to reach a level of certainty for the potential injury which may be caused by the amendments. It compares Indian court rulings on privacy rights to the taxonomy of privacy harms. From this we gain knowledge of the types of privacy injuries which have been protected by law in India. An insight is also gained into the general approach of the courts in granting relief in cases involving questions of privacy law. Part III, then examines sections 69 and 69B which provide the power to issue directions for intercepting data and monitoring and storing information respectively. These sections are analysed against the regulations made under section 5(2) of the Telegraph Act. A quick review demonstrates that sections 69 and 69B provide for adequate safeguards when viewed against the standards set by precedent. Part IV contends that even with these safeguards and procedures, the protection of privacy rights is inadequate in view of the inherent lack of incentive to observe procedure and the nature of internet communications. The types of harms caused due to the new measures as well as the lack of incentive to observe the procedure presents a real and present danger to the right to privacy. The final part of the article tersely suggests that *ex-ante ex-parte* court orders are a standard that should be explored in relation to breach of privacy in internet communications.

II

THE RIGHT TO PRIVACY RECENTLY

A. THE TAXONOMY OF PRIVACY

It is obligatory to cite the seminal twenty seven page article authored by Warren and Brandis[19] which developed the modern contours of the tort of privacy. The article sparked a renaissance of

---

[17] *See, e.g.,* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("[p]rivacy is... the control we have over information about ourselves."); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151 (2004).

[18] *See* Diljeet Titus v. Alfred A. Adebare, 130 (2006) D.L.T. 330 (India) (*Per* Sanjay Kishan Kaul, J.) (a case for the grant of an injunction on allegations of theft of data, copyright infringement and theft of trade secrets). The present article does not substantially discuss these areas of law which touch upon the periphery of the privacy harm of information dissemination. I consider these areas of law, when applied to privacy rights, to be subsidiary and of limited assistance to a person.

[19] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197 (1890) (seizes upon the metaphor of 'man's house as his castle' to call for a common law right to privacy).

legal scholarship and subsequently neighbouring theories were devised to defend the right to privacy.[20] Much ink and paper have been sacrificed to etch out the development of the right to privacy, and it is outside the scope of the present article to present each of them.[21]

For the purposes of the present article, I utilize the taxonomies of privacy harms developed by two influential thinkers. The first is the one proposed by Prosser, according to whom four distinct torts flow from a breach of privacy: (a) intrusion upon a person's solitude or seclusion or into his affairs; (b) public disclosure of embarrassing facts of a person's private life; (c) publicity which places an individual in false light in public eyes; and (d) appropriation to a person's advantage of another's name or likeness.[22] This four tort classification has received acceptance,[23] being adopted by the First Restatement of Torts and different state legislatures and courts across the United States.[24]

The second taxonomy devised by Daniel J. Solove[25] is of a more recent origin and has become the popular norm to gauge the types of privacy harms in the internet age.[26] The author categorises the privacy harms as falling into four distinct categories: (a) information collection, (b) information processing, (c) information dissemination, and (d) invasion.[27] The author further breaks down these broad classifications into sub-categories to address each form of harm which is being caused

---

[20] *See, e.g.,* Roscoe Pound, *Interests in Personality*, 28 HARV. L. REV. 343 (1915); Erwin N. Griswold, *The Right to Be Let Alone*, 55 NW. U. L. REV. 216 (1960).

[21] Ken Gormley, *One Hundred Years of Privacy*, WIS. L. REV. 1335 (1992) (overviews the legal scholarship on the subject of privacy law and concludes that a simple or precise definition of the right to privacy is a 'misguided quest' and the law will keep evolving with new permutations).

[22] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (argues that the invasion of privacy in fact consists of four distinct torts).

[23] Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006 (High Court of Delhi, 12th October 2007) (India), at ¶ 74 (*Per* Gita Mittal, J.) (a suit for injunctive relief to prevent the defendant from publishing the plaintiff's name in the Forbes list of Indian billionaires on the grounds of a breach of the right to privacy); *see also, e.g.,* Union of India v. United India Insurance, (1997) 8 S.C.C. 683 (India), at ¶ 10 (*Per* S.B. Majmudar & M. Jagannadha Rao, JJ.); Kaleidoscope (India) Pvt. Ltd. v. Phoolan Devi, A.I.R. 1995 Del. 316 (India), at ¶ 9 (*Per* M. Jagannadha Rao, C.J. & D.K. Jain, J.); P. Mukundan v. Mohan Kandy Pavithran, (1992) I.I.L.L.J. 160 Ker. (India), at ¶ 22 (*Per* K. Sukumaran & L. Manoharan, JJ.).

[24] Alexandra B. Klass, *Tort Experiments in the Laboratories of Democracy*, 50 WM. & MARY L. REV. 1501, 1526 (2009) (surveys how influential modern torts evolved and were introduced in the U.S. legal system).

[25] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 482-483 (2006) (stating that the state of privacy law is in disarray and the objective of the article is to codify it, to make sense of the harms caused by a breach of privacy).

[26] *See* Scott Michelman, *Who Can Sue Over Government Surveillance?*, 57 UCLA L. REV. 71 (2009); Flora J. Garcia, *Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 693 (2007); Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L. J. 55 (2007).

[27] *Supra* note 25, at 489.

to the right to privacy. The first category of information collection consists of surveillance and interrogation. The next category is information processing which involves taking the information gathered and making sense out of the raw facts for any probable use which has been classified by the author into aggregation, identification, insecurity, secondary use and exclusion. The third category is concerned with the dissemination of the information and it consists of the breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion. The final category is concerned with invasion which the author defines as concerning invasive acts that disturb one's tranquillity or solitude without concerning information.[28] These classifications shall be used throughout this article to get a sense of the privacy harms which are inflicted by the powers which are vested under sections 69 and 69B.

B. LIMITED RECOGNITION OF HARMS

Contrary to the communal notions of Indian society,[29] courts have often had the occasion to touch upon the various aspects of the right to privacy.[30] This has been necessitated by the absence of any general enactment granting the right to privacy.[31] Though other countries may join India on this position, India, till recently, remained one of the few not to have any created sector specific laws relating to technology.[32] However, this has not stopped citizens from approaching courts and

---

[28] *Supra* note 25, at 483.

[29] Bhikhu Parekh, *Private and Public Spheres in India*, 12 CRITICAL REV. INT'L SOC. & POL. PHIL. 313, 317 (2009) ("[I]ndians do not place much value on individual autonomy. Although the latter has begun to enter Indian life and exercises varying degrees of influence on different sections of society and in different areas, its reach remains rather limited and its impact uneven."); *see also* Court on its motion v. Union of India, 139 (2007) D.L.T. 244 (India), at ¶ 8 (*Per* Swatanter Kumar & H.R. Malhotra, JJ.). Urban India seems to be ascribing a value to privacy. A recent court prohibition evidences this trend. The prohibition was imposed on black films put on the windscreens of cars by owners for privacy as well as to shield them from the sun, on the ground that this was being used by criminals to perpetrate offences, often rape and molestation in moving vehicles.

[30] *See, e.g.,* Jamuna Prasad & Ors. v. Lachman Prasad, (1888) I.L.R. 10 (All.) 162 (India) (*Per* John Edge, Kt., C.J. & Brodhurst, J.) ("[a]s to the objections, the findings on remand show that the plaintiff is entitled to have his right of privacy observed, and to have a mandatory order to compel the appellant to permanently close the door or window complained of."); *see contra* Sayyad Azuf v. Ameerubibi, (1895) I.L.R. 18 (Mad.) 163 (India) (*Per* Muttusami Ayyar & Best, JJ.). There is a catena of early cases where the right to privacy has been in issue. This challenges the conventional notion that Indians have been non-litigious on privacy. However, these cases are centred towards easementary squabbles.

[31] *See* ABRAHAM L. NEWMAN, INTERNATIONAL DATA PRIVACY LAWS AND THE PROTECTORS OF PRIVACY 29 (2008). General laws on privacy are not always desirable. The author notes that comprehensive data protection regimes have a chilling effect on business. This is explained with the example of the absence of the subprime mortgage market in countries which have comprehensive and general laws due to credit information sharing regulations.

[32] *See* Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?*, 21 TEMP. INT'L & COMP. L.J. 103, 111-113 (2007).

alleging breach of privacy.[33] These were often complaints against unwanted state intrusion,[34] thereby giving the Indian Supreme Court occasion to constitutionalise the tort of privacy reading it under an expansive interpretation of the right to life.[35] Hence, in the absence of a general law governing privacy, the law of privacy in India has been developed through precedent. The classifications presented above are of little use without putting them in the context of privacy law recognized and enforced in India.

The Indian Supreme Court's decision in *Gobind*,[36] reintroduced the right to privacy into the Indian legal system. The constitutional holding that frequent domiciliary visits by the police without a reasonable cause infringed upon the petitioners' right to privacy firmly established the right for citizens of the country.[37] This form of breach of privacy has remained most popularly contested by litigants and guarded by courts. Hence both Prosser's and Solove's first classifications of privacy harms find reflection in Indian law. The law developed in cases of 'intrusion upon a person's solitude or seclusion' and 'information collection' has been applied across the spectrum of privacy harms.[38]

---

[33] *See* R. Rajagopal v. State of Tamil Nadu, A.I.R. 1995 S.C. 264 (India) (*Per* B.P. Jeevan Reddy and Suhas C. Sen, JJ.) (hereinafter '*Rajagopal*') ("[t]his right has two aspects which are but two faces of the same coin, (1) the general law of privacy which affords a tort action for damages resulting from an unlawful invasion of privacy, and (2) the constitutional recognition given to the right to privacy which protects personal privacy against unlawful governmental invasion."). The tort of privacy has had a stunted development in India. The recent development of the right has constitutional origins, which has revitalised the tort of privacy.

[34] M.P. Sharma v. Satish Chandra, (1954) 1 S.C.R. 1077 (India) (*Per* Mehr Chand Mahajan, C.J. et al.) (rejected a right to privacy argument that a search warrant issued as per section 96(1) of the Code of Criminal Procedure, 1898 would be *ultra vires* Arts. 19(1)(f) & 20(3) of the Constitution of India); Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295 (India) (Subha Rao, J., dissenting) (concerned a challenge to the constitutionality of Rule 236 of the U.P. Police Regulations).

[35] Gobind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148 (India) (*Per* K. K. Mathew, J. et al.) (holding that unnecessary domiciliary visits and picketing were a breach of the petitioner's right to privacy); Malak Singh v. State of Punjab & Haryana, (1981) 1 S.C.C. 420 (India) (upholding the constitutional validity of maintaining 'history sheets' under the Police Act and the Punjab Police Rules); *see generally* Griswold v. Connecticut, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The development is opposite to that of the US Supreme Court where first the tort of privacy was endorsed and then subsequent efforts were made to incorporate it into the ambit of the Fourth Amendment.

[36] Gobind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148 (India).

[37] *See, e.g.,* Khushwant Singh v. Maneka Gandhi, A.I.R. 2002 Del. 58 (India) (*Per* Devinder Gupta & Sanjay Kishan Kaul, JJ.); Elkapalli Latchaiah v. Govt. of Andhra Pradesh, 2001 (5) A.L.D. 679 (India) (*Per* S. B. Sinha, C.J. & V. V. S. Rao, J.); Tamil Nadu Tamil & English Schools Association v. State of Tamil Nadu, 2000 (2) C.T.C. 344 (*Per* A. S. Venkatachalamoorthy, J. et al.).

[38] *Supra* note 22; *supra* note 25.

The second classification proposed by Solove is absent from precedent. Indian courts have not had the occasion to adjudicate upon issues of information processing as it seems to have not been averred. Persons when alleging a breach of their privacy are more concerned with the interception and the dissemination of private information and seem to have glossed over agitating about their rights against information processing.[39] Moreover, it seems that courts have held that any information existing in the public domain can be processed and then published. Here, the moment the information leaves the absolute control of the person, the information can be used by another.[40]

Disclosure is one aspect where courts have zealously guarded the right to privacy. Claims for unauthorized disclosure breaching a right to privacy have more often than not been entertained by courts.[41] There also exist legislative provisions which grant privacy in a specified class or people or

---

[39] Asahi Glass India v. Director General of Investigation and Registration, WP(C) 8741/2008 (High Court of Delhi, 25th September 2009) (India) (*Per* Sanjiv Khanna, J.). The petitioner sought to quash inquiry proceedings initiated against it on allegations of cartelization. The petitioner contended amongst other things that the inquiry would result in a breach of privacy as section 49 of the Monopolies and Restrictive Trade Practices Act, 1969 would obligate it to furnish information threatening its privacy. The court held that the aforementioned section contained an exception – the petitioner could refuse to provide information pursuant to a 'reasonable excuse' being proved; *see* A. Raja v. P. Srinivasan, (2009) 8 M.L.J. 513 (India) (*Per* M. Chockalingam & R. Subbiah, JJ.). The applicant sought to restrain the respondent, the publisher of a weekly, from publishing *inter alia,* family photographs of the applicant accompanied by write ups leveling allegations of corruption. The appellant had contended that these photographs contained images of his wife and minor child who were not connected to his public office and public acts and hence the publication of their images contemporaneously infringed their right to privacy. The court granted an interim injunction restraining the defendant from publishing any such news articles as well as photographs of the plaintiff's wife and minor child.

[40] Petronet LNG Ltd. v. Indian Petro Group, (2009) 95 S.C.L. 207 (Delhi) (India) (*Per* S. Ravindra Bhat, J.). The case concerned an application for an injunction against the defendants from publishing information which the plaintiff alleged was confidential. The plaintiff alleged that the defendant breached its privacy by accessing as well as disseminating information. The court held that the information was freely available in public and hence the defendant was not in breach of the plaintiff's right to privacy; s*ee also* Rajinder Jaina v. Central Information Commission, 164 (2009) D.L.T. 153 (India) (*Per* Sanjiv Khanna, J.). The case concerned a writ petition about the disclosure of information under the Right to Information Act, 2005 wherein the petitioner challenged the disclosure on grounds of infringement of the right to privacy. The court held that the information already existed in the public domain and no claims as to privacy could be made. The court also applied the ratio laid down in *Rajagopal* whereby the Court held that once a matter becomes an issue of public record, no privacy can be claimed for it.

[41] S*ee, e.g.*, Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006 (High Court of Delhi, 12th October 2007) (India) (*Per* Gita Mittal, J.). The court noted in paragraph 57 that the enforcement of the right to privacy under the Indian constitutional scheme can only be made against state instrumentalities and not against private persons. After this holding, the Court in paragraph 58 examined the poor growth of the right to privacy as a tort in India. The court after examining the precedent in the United Kingdom held the same to be inapplicable. It hinted in paragraphs 66 & 67 that despite the absence of any statute granting a right to privacy, the guidelines laid down by the Supreme Court in *Rajagopal* develop such a right; *see also* Managing Director, Makkal Tholai v. Mrs. V. Muthulakshmi, (2007) 5 M.L.J. 1152 (India) (*Per* P. Jyothimani, J.). The case concerned an application for an

circumstances.[42] Here courts seemed to have recognized the right arising from a relationship between the parties where information is shared by a person voluntarily; however it is done with another only in the bounds of the bilateral relationship.[43] Hence, the second classification suggested by Prosser and the third classification suggested by Solove find recognition in Indian law. However, the discrete harms which are classified by Solove are yet to evolve or be appreciated by Indian Courts. Courts generally examine (a) the existence of a person's right to privacy; (b) the conduct of another causing a breach into the privacy; and (c) whether such a breach is legally permissible. This is a limited appreciation of evolving new types or subcategories of harms for applying distinct judicial norms. Hence, there is no effective rule creation appreciating the differing nature of privacy harms. To conclude the Indian legal system has yet to give recognition to most harms flowing from breaches of privacy and broadly recognizes only the harms arising from information gathering and disclosure.

III

ONLINE PRIVACY: PAST, PRESENT AND ABSENT

A. INFORMATION GATHERING

1. General rules for information gathering

The ever increasing reach of the internet was belatedly realized by the Indian legislature in 2001[44] and it has been playing a game of catch up ever since.[45] However, regulations pertaining to privacy were largely absent from the statute.[46] In a telling analogy of legislative lethargy one finds that rules

---

injunction filed by the respondent, the widow of the infamous outlaw Veerappan, against the defendants, in order to prevent the defendants from telecasting a television serial on his life.

[42] § 327(1), Code of Criminal Procedure, 1973, No. 2 of 1974; §§ 3 & 4, Indecent Representation of Women (Prohibition) Act, 1986, No. 60 of 1986; § 7(1)(c), Medical Termination of Pregnancy Act, 1971, No. 34 of 1971; § 21, Juvenile Justice (Care and Protection of Children) Act, 2000, No. 56 of 2000. These statutory provisions protect women and children from publicity in certain circumstances. However, they only afford an extremely thin level of protection.

[43] *See* Vijay Prakash v. Union of India, A.I.R. 2010 Del. 7 (India) (*Per* S. Ravindra Bhat, J.). After considering the English law on the point of privacy, the court notes that, "it may be seen from the above discussion, that originally, the law recognized relationships through status (marriage) or arising from contract (such as employment, contract for services, etc.) as imposing duties of confidentiality."

[44] *See* APAR GUPTA, COMMENTARY ON THE INFORMATION TECHNOLOGY ACT, 2000 3-4 (LexisNexis Butterworths Wadhwa 2007) (observes the introduction of the law and its eventual passage).

[45] *See* DEPARTMENT OF INFORMATION TECHNOLOGY, MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA, REPORT OF THE EXPERT COMMITTEE ON PROPOSED AMENDMENTS TO INFORMATION TECHNOLOGY ACT 2000, (2005), *available at* http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/ITAct.doc.

[46] *See* § 72, Information Technology Act, 2000, No. 21 of 2000.

for interception of telecommunications were only framed in 1999[47] after the Supreme Court decision in *PUCL v. Union of India*.[48] These rules provide the blueprint for the interference with privacy rights for 'intrusion upon a person's solitude or seclusion' and 'information collection.'[49] These rules are the close mirrors to the rules which have recently been enacted under sections 69[50] and 69B.[51]

The rules for interception of telecommunications have been framed under section 5(2) of the Telegraph Act which provides that when (a) public emergency; or (b) public safety situation exists, then an order may be made to issue directions for interception. These rules effectively authorize high ranking public functionaries[52] to issue directions for the interception of messages.[53] To safeguard against a blanket infraction of civil liberties, the section itself provides for several safeguards. There are documentary formalities with which the officials have to comply.[54] These are essentially the recording of reasons in the nature of (a) interests of sovereignty and integrity of India; (b) the security of the state; (c) friendly relations with foreign states; (d) public order; and (e) incitement to the commission of an offence.[55]

There are several safeguards which have been added by the regulations to augment the section under Rule 419-A of the Indian Telegraph Rules. These are firstly in the nature of providing more specifics to the documentary formalities such as providing the particulars of the officer directing the interception and the maintenance of records.[56] Secondly, there is limited regulatory oversight

---

[47] Indian Telegraph (First Amendment) Rules, 1999 (G. S. R. 123(E)) (Feb. 16, 1999) (even though the Indian Telegraph Act was enacted in 1885 from which time it has permitted the interception of communications).
[48] People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India) (concerned the legality of telephone tapping).
[49] Rule 419-A(3), Indian Telegraph Rules, 1951.
[50] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (G. S. R. 780(E)) (Oct. 27, 2009).
[51] Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (G. S. R. 782(E)) (Oct. 27, 2009).
[52] Rule 419-A(1), Indian Telegraph Rules, 1951.
[53] Rule 419-A(3), Indian Telegraph Rules, 1951.
[54] State v. Mohd. Afzal & Ors, 107 (2003) D.L.T. 385 (India) (*Per* Usha Mehra & Pradeep Nandrajog, JJ.) ("[p]ermission was taken from the Joint Director, Information & Broadcasting on 13.12.2001 itself for interception... as reflected in the order dated 11.7.2002 these were produced in a sealed cover which was opened, contents read out to the accused and their counsel and then resealed.").
[55] § 5(2), Indian Telegraph Act, 1885, No. 13 of 1885.
[56] Rules 419-A(6) & (7), Indian Telegraph Rules, 1951.

which has been built up in the section in the form of a review committee.[57] Thirdly, the final safeguard is an automatic expiry on the interception direction on ninety days being completed.[58]

In public law cases, especially involving the first taxonomy of 'intrusion upon a person's solitude' or 'information gathering,' the approach adopted by courts has been one of applying the constitutional doctrines developed under Articles 14, 19 and 21.[59] These doctrines permit the judiciary to strike down a statute which is deemed unreasonable or which does not have any connection to the object of the legislation; yet there has been hesitation on the part of the courts to do so. The protection which has been afforded to individuals has been restricted to a strict adherence to the procedural safeguards in law. The courts have termed the right to privacy as, 'too broad and moralistic.'[60] They have shied away from substantively limiting the power of the state and have rather insisted on procedures being adhered to. This trend is exposed by the celebrated case of *PUCL v. Union of India* where the Supreme Court laid down procedural safeguards in the form of directions to check warrantless telephone tapping.[61] Recent precedent further evidences this trend. In a case relating to the constitutional validity of telephone tapping provisions of MCOCA, the Supreme Court has held that the provisions prescribe adequate procedural safeguards.[62] Again in a case dealing with the powers of the CBI, Justice Sinha has remarked that it would be desirable for them to evolve safeguards.[63]

---

[57] Rule 419-A(8), Indian Telegraph Rules, 1951.

[58] Rule 419-A(5), Indian Telegraph Rules, 1951.

[59] T. R. Andhyarujina, *The Evolution of the Due Process of Law by the Supreme Court*, *in* SUPREME BUT NOT INFALLIBLE: ESSAYS IN HONOUR OF THE SUPREME COURT OF INDIA 203 (B. N. Kirpal et al. eds., 2004).

[60] *See, e.g.,* Neera Agarwal v. Mahender Kumar Agarwal, 2009 (5) A.L.T. 518 (India), at ¶ 61 (*Per* P. S. Narayana, J.); Surupsingh Hrya Naik v. State of Maharashtra, A.I.R. 2007 Bom. 121 (India), at ¶ 11 (*Per* F. I. Rebello & R. M. Savant, JJ.); Rajesh Kumar v. State of U.P., 1999 Cri.L.J. 2388 (All.) (India), at ¶ 72 (*Per* Binod Kumar Roy & R. K. Singh, JJ.).

[61] *Supra* note 48.

[62] State of Maharashtra v. Bharat Shanti Lal Shah, (2008) 13 S.C.C. 5 (India) (*Per* K. G. Balakrishnan, C.J. et al.). The case mainly concerned the constitutional competence of the state to enact sections 13-16 of the Maharashtra Control of Organised Crime Act, 1999. The court observed at paragraph 60, "interception of conversation though constitutes an invasion of an individual right of privacy but the said right can be curtailed in accordance with procedure validly established by law. Thus, what the court is required to see is that the procedure itself must be fair, just and reasonable and non-arbitrary, fanciful or oppressive."

[63] Bhavesh Jayanti Lakhani v. State of Maharashtra, 2009 (9) S.C.A.L.E. 467 (India), at ¶ 133-134 (*Per* S. B. Sinha & Mukundakam Sharma, JJ.). The court dealing with the powers of the Central Bureau of Investigation under the Extradition Act, 1962 held that, "[n]o such guideline, however, has been laid down in respect of surveillance conducted pursuant to a Red Corner or Yellow Corner Notice... the Central Government and in particular the Ministry of External Affairs, in our opinion, should frame appropriate guidelines in this behalf."

2. Section 69 of the Information Technology Act, 2000

After much discontentment and debate,[64] the Information Technology Act, 2000 received its first major amendment in 2008.[65] The Amendment Act sought to rectify the many deficiencies which had been noticed with the application of the enactment.[66] The amendment sought to make the Information Technology Act, 2000 a self sufficient act with respect to internet behaviour.[67] Hence the legislature introduced section 69.[68] Section 69 is titled the "power to issue directions for interception or monitoring or decryption of any information through any computer resource." The section mirrors section 5(2) of the Telegraph Act, containing the same limitations on the exercise of the power to issue directions. It contains a similar structure adhering to the constitutional limitations as prescribed in *PUCL*,[69] where the direction may only be issued when a) public emergency; or (b) public safety situations exist. It also contains the requirement of recording reasons for issuing the direction and mentioning the 5 classes of events as contained in section 5(2). It does not cause surprise that the recent regulations prescribed under section 69(2) for providing the procedure for issuing directions also broadly follow Rule 419-A. They mirror most of the procedural safeguards of documentary adherence, oversight and automatic expiry.

3. Section 66E of the Information Technology Act, 2000

Curiously the amendment also brings forward a section titled "punishment for violation of privacy." Though, the title of the section is worded broadly it seeks to apply only to capturing[70] an "image of the private area of a person", "under circumstances violating the privacy of the person."[71] The circumstances violating the privacy of a person are when such person has a reasonable expectation that (a) he or she could disrobe in privacy without being concerned that an image of

---

[64] *See* Editorial, *Plugging IT Loopholes*, HINDU BUS. LINE, Sept. 6, 2005, *available at* http://www.blonnet.com/2005/09/06/stories/2005090600061000.htm.

[65] Information Technology (Amendment) Act, 2008, No. 10 of 2009.

[66] UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT (United Nations 1999), *available at* http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf. The practical difficulties were natural since the Information Technology Act, 2000 which was derived from the UNICITRAL Model Law was never fully adapted as a general enactment to govern internet behaviour.

[67] Information Technology (Amendment) Act, 2008, No. 10 of 2009 (contains 49 numbered paragraphs which contain insertions, substitutions and deletions to several sections of the Information Technology Act, 2000).

[68] *Id.*

[69] *Supra* note 48.

[70] § 66E, Information Technology Act, 2000, No. 21 of 2000. The rules equally apply to publishing and transmitting. Hence, there is recognition of the harm of information dissemination in the section, with the same amount of liability imposed on the offender for capturing, publishing or transmitting.

[71] § 66E (1), Information Technology Act, 2000, No. 21 of 2000.

his/her private area was being captured; or (b) any part of his/her private area would not be visible to the public, whether such person is in a public or a private place.[72]

B. INFORMATION PROCESSING

Though styling itself to be concerned properly with the processing of information, section 69B is a hybrid between information gathering and processing.[73] The section is titled "power to authorize to monitor or collect traffic data or information through any computer resource for cyber security." The section's objectives are essentially better internet management with the specific mandate of "enhancing cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant."[74] Towards this goal the section allows for issuing directions to "monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource."[75] A review of the regulations formed under the section make it clear that the harms which will be incurred are in the nature of information processing, such as aggregation and identification.[76] The section provides similar safeguards as found in section 69, but the conditions for exercise of the power are entirely different. Due to this, the reasons which have to be recorded are not on the high thresholds which are set under section 69.[77] These are the reasons which have been enunciated under the *PUCL* case. Hence, there lies an argument against the constitutionality of the section as the regulations formed under it clearly contemplate independent directions to monitor data, which as a technical pre-requisite necessarily requires interception.

C. INFORMATION DISCLOSURE/DISSEMINATION

1. Conventional treatment of information disclosure/dissemination

What further complicates the mix of privacy injuries is the nature of the information. Information which lies at the root of privacy in all cases is not the same. It deals with different scope of human activities and a breach into the privacy of each incurs a different grade of harm. The law of information disclosure has developed most with respect to the freedom of press. Here, claims have

---

[72] § 66E, Explanation (e), Information Technology Act, 2000, No. 21 of 2000.
[73] § 69B, Information Technology Act, 2000, No. 21 of 2000.
[74] *Id.*
[75] § 69B, Information Technology Act, 2000, No. 21 of 2000.
[76] Rule 3(4), Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 ("may include the monitoring of data or information for any person or any class of persons.").
[77] Rule 3(2), Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (contains the different types of situations which can threaten cyber security).

often been made that the publication of facts harms the privacy of person in society.[78] These claims are often intertwined with the law of defamation, when the person disputes the veracity of the information sought to be disclosed.[79] Then there are cases where examining the information for which a breach is complained against arise from a fiduciary relationship. Irrespective of the doctrinal origins arising from tort or from Part III of the Constitution, Courts generally adopt a methodology to judge such cases. Courts gauge (a) the source of the information, such as fiduciary relationships e.g. doctor-patient,[80] matrimonial,[81] and bank-customer,[82] and (b) the contents of the information, e.g. presence of the AIDS virus,[83] a spouse's infidelity,[84] and failure to pay debts.[85] Here, courts balance the countervailing arguments for public benefit which may arise from the disclosure. Courts, hence, may allow the disclosure when it concerns a person infected with the AIDS virus whose prospective marriage will likely result in the communication of the virus;[86] the issue of the legitimacy of a child for which a divorced husband will be liable to pay maintenance;[87]

---

[78] *See, e.g.,* R. Sukanya v. R. Sridhar, A.I.R. 2008 Mad. 244 (India) (*Per* S. Manikumar, J.) (holding that publication of proceedings in a family court meant to be in-camera will affect the constitutional liberty guaranteed to the individual and it would be an invasion of his right of privacy).

[79] *See* Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006 (High Court of Delhi, 12th October 2007) (India), at ¶ 74 (*Per* Gita Mittal, J.); Khushwant Singh v. Maneka Gandhi, A.I.R. 2002 Del. 58 (India) (*Per* Devinder Gupta & Sanjay Kishan Kaul, JJ.).

[80] Mr. 'X' v. Hospital 'Z', (1998) 8 S.C.C. 296 (India) & (2003) 1 S.C.C. 500 (India) (involved a claim for damages made by a patient against a hospital which disclosed the fact that the patient tested positive for HIV which resulted in his proposed marriage being called off and the patient being ostracized by the community).

[81] Akila Khosla v. Thomas Mathew, 2002 (62) D.R.J. 851 (India) (*Per* V. S. Aggarwal, J.); *see also* Premkumar v. Rajeswari, CrlRC 1095/2007 (High Court of Madras, 8th October 2009) (India) (*Per* T. Sudanthiram, J.). The case concerned an appeal against a decision in maintenance proceedings denying the appellant's request for a DNA test of the offspring of the respondent, which the appellant claimed was not born out of wedlock but from an adulterous affair. The Court applying the decision of the Supreme Court in *Sharda v. Dharmpal*, 2003 (2) C.T.C. 760 (India), held that though a DNA test may be invasive of the respondent's right to privacy, it may be permitted in maintenance proceedings when it was the only way of leading evidence for the appellant's contention that since the child was the result of adultery, they were not liable to pay maintenance for the child.

[82] Mr. K. J. Doraisamy v. The Assistant General Manager, State Bank of India, (2006) 4 M.L.J. 1877 (India) (*Per* V. Ramasubramaniam, J.). The petitioner, who was a defaulting borrower, challenged the power of the banks to publish his photograph in newspapers as offending his right to privacy.

[83] *Supra* note 80.

[84] Akila Khosla v. Thomas Mathew, 2002 (62) D.R.J. 851 (India) (*Per* V. S. Aggarwal, J.).

[85] *Supra* note 81.

[86] *Supra* note 82.

[87] *Supra* note 84; *see contra* Rayala M. Bhuvaneshari v. Nagaphanender Rayala, A.I.R. 2008 A.P. 98 (India) (*Per* Bilal Nazki, J.) *aff'd in*, Neera Agarwal v. Mahender Kumar Agarwal, 2009 (5) A.L.T. 518 (India). Without the knowledge of the wife, the husband tapped the conversations of the wife with third parties. The court held that the privacy of the wife was clearly infringed by this act and that any such evidence gathered by the husband would be inadmissible as evidence.

and the steps to be taken by a bank to recover debts from a wilful defaulter.[88] Recently, an impressive body of law has also developed in relation to the recently enacted Right to Information Act, 2005.[89]

2. Protection against online dissemination

Pre-amendment, the Information Technology Act provided a shade of privacy protection to guard against unwarranted disclosure. These were provisions in the nature of prohibition of disclosure of information gathered in the course of performance of functions mandated under the Act.[90] Continuing this approach, the amendment added several sections which seek to guard against the disclosure of information which is gathered in the course of their functions. These include section 43A for compensation which a body corporate will be liable to pay for the failure to protect 'sensitive personal data or information.'[91] Even the regulations which have been framed under sections 69 and 69B provide for stringent sanctions against the disclosure of information which is gathered by intermediaries and persons employed by them. What is interesting is that these regulations go beyond the regulations on telecommunications insofar as providing for affirmative duties on intermediaries as well as penal sanctions for non-adherence. These are mostly in the nature of protecting strict confidentiality with the data and provide for penal sanctions. The second area where the dissemination of information is prohibited pertains to obscene materials and paedophilia. These are not analyzed for the causal ingredient since for the prohibition it is the existence of 'obscenity' and not a breach of privacy that is vital. Hence, they cannot be properly considered as legislative measures to protect the privacy harms of information dissemination.

---

[88] *Supra* note 82. The court held that, "if borrowers could find newer and newer methods to avoid repayment of the loans, the banks are also entitled to invent novel methods to recover their dues." *See also* District Registrar & Collector, Hyderabad v. Canara Bank, A.I.R. 2005 S.C. 186 (India). The case involved a constitutional challenge by the banks to the powers of search and seizure provided to any person authorized by the collector under an amendment to the Stamp Act, 1899 for the purposes of discovering any material in relation to the evasion of stamp duty. The court opined in paragraph 34, "the legislative intrusions must be tested on the touchstone of reasonableness as guaranteed by the constitution and for that purpose the court can go into the proportionality of the intrusion vis-à-vis the purpose sought to be achieved."

[89] Union of India v. Central Information Commission, WP(C) 16907/2006, 3607 & 7304/2007, 4788 & 6085/2008 & 7930, 8396 & 9914/2009 (High Court of Delhi, 5th January 2010) (India) (*Per* Sanjiv Khanna, J.). The case concerned a challenge to the refusal of the Central Information Commission to divulge information under the Right to Information Act, 2005. The challenge involved an interpretation of section 8(1)(j) of the aforementioned statute which sought to restrict the disclosure of information under the Act when it, "would cause unwarranted invasion of the privacy of the individual" unless the respondent held that such disclosure could be made in 'larger public interest.' *See* Rajinder Jaina v. Central Information Commission, 164 (2009) D.L.T. 153 (India) (*Per* Sanjiv Khanna, J.).

[90] § 72, Information Technology Act, 2000, No. 21 of 2000.

[91] Explanation (iii), § 43A, Information Technology Act, 2000, No. 21 of 2000.

IV

THE LIMITATIONS OF THE PRESENT PRIVACY REGIME

A. DESIGN DEFECTS IN THE PRESENT SURVEILLANCE REGIME

1. Lack of incentive, a lack of procedure

There are several inherent problems in the application of the present legal regime. A review of court decisions has demonstrated that even though courts apply due process, they have heavily relied upon first framing strict procedures and have demanded an adherence to them to gauge the legality of telephone tapping. In all probability, the same approach will be adopted towards online surveillance.

The most obvious criticism which may be levelled against 'the privacy through procedure argument' will be that people will simply not comply with such procedure. Such a counter will posit that bureaucrats and police officials put in charge of the safeguards will hardly be sticklers for procedures. Their primary job will be policing and not securing the privacy of citizens. Hence, they will bring an institutional bias to their function.[92] The counter finds its logical end by making a lack of incentive argument. It states that the authorities will bring to the job an unabated enthusiasm to secure a conviction and will view the safeguards provided in the statute as hurdles to their goals. A review of the decisions will show that courts have without hesitance convicted offenders on evidence gathered by improper procedure when such procedure is often held not mandatory.[93] The deficiency in observing the safeguards for telephone tapping has been held by the Supreme Court to not affect the admissibility of the evidence.[94] The Court held that –

---

[92] M. P. JAIN & S. N. JAIN, PRINCIPLES OF ADMINISTRATIVE LAW 225-234 (2002); *see* Romesh Sharma v. State of Jammu & Kashmir, 2007 (1) J.K.J. 84 (India) (*Per* Y.P. Nargotra, J.). The court appreciated arguments as to the institutional bias against the vigilance organisation of the state police, where the evidence which had been gathered by the vigilance organisation from the accused petitioner on a case was stolen. Thereafter, another criminal investigation was commenced by the vigilance organisation. The petitioner fearing his false implication in the case of the theft alleged institutional bias and the court ordered that the investigation of the theft be transferred to an independent third entity. *See also* South Indian Cashew Factories Workers' Union v. Managing Director, (2006) 5 S.C.C. 201 (India) (*Per* Arijit Pasayat & Tarun Chatterjee, JJ.). It was held that the inquiry had been conducted by the Assistant Personnel Manager of the Corporation and the Union raised an industrial dispute in which the Labour Court set aside the inquiry on the ground of institutional bias as the Enquiry Officer was part of the same institution and had also made certain uncorroborated remarks against the employee.

[93] R. M. Malkani v. State of Maharashtra, A.I.R. 1973 S.C. 157 (India). The court deciding on the admissibility of evidence under section 7 of the Evidence Act, 1972 held that, "...there is warrant for the proposition that even if evidence is illegally obtained it is admissible. Over a century ago it was said in an English case where a constable searched the appellant illegally and found a quantity of the offending article in his pocket that it would be a dangerous obstacle to the administration of justice if it were held, because evidence was obtained by illegal means, it could not be used against a party charged with an offence. *See* Jones v. Owen, (1870) 34 JP 759..." *See also* Saiyad Mohammad Saiyad Umar Saiyad v. State of Gujarat, (1995) 3 S.C.C. 610 (India); C. Ali v. State of Kerala, (1999) 7 S.C.C. 88 (India);

> In regard to the first aspect, two infirmities are pointed out in the relevant orders authorizing and confirming the interception of specified telephone numbers. It is not shown by the prosecution that the Joint Director, Intelligence Bureau who authorized the interception, holds the rank of Joint Secretary to the Government of India. Secondly, the confirmation orders passed by the Home Secretary (contained in volume 7 of lower Court record, Page 447 etc.) would indicate that the confirmation was prospective. We are distressed to note that the confirmation orders should be passed by a senior officer of the Government of India in such a careless manner, that too, in an important case of this nature. However, these deficiencies or inadequacies do not, in our view, preclude the admission of intercepted telephonic communication in evidence. It is to be noted that unlike the proviso to Section 45 of POTA, Section 5 of the Telegraph Act or Rule 419A does not deal with any rule of evidence. The non-compliance or inadequate compliance with the provisions of the Telegraph Act does not *per se* affect the admissibility.[95]

Hence, when the function is exercised with a bias towards conviction and there is a lack of incentive, these procedures will be routinely flouted. It cannot be said that the mere vesting of this discretion will lead to a presumption that it will be exercised with an evil eye and an unequal hand.[96] However, the regulations are designed in a manner where there is a deep seated bias towards securing conviction with or without an adherence to procedure.

State of Punjab v. Baldev Singh, (1999) 6 S.C.C. 172 (India); Beckodan Abdul Rahinan v. State of Kerala, (2002) 4 S.C.C. 229 (India). These cases concern the admissibility of evidence gathered in a manner that is not compliant with the procedural safeguards set out in section 50 of the Narcotic Drugs and Psychotropic Substances Act, 1985. The courts have held that only if the safeguards are mandatory shall non-compliance render the evidence inadmissible.

[94] State (N.C.T. of Delhi) v. Navjot Sandhu, A.I.R. 2005 S.C. 3820 (India) (*Per* P. Venkatarama Reddi & P.P. Naolekar, JJ.).

[95] *Id.* at ¶ 16. It is to be noted that even though the Information Technology Act, 2000 does not contain a section analogous to section 45 of the Prevention of Terrorism Act, 2002 which contained language to make evidence admissible even in cases of procedural impropriety for which the decision was given, the general approach of law enforcement is to flout procedural safeguards. *See also* K. L. D. Nagasree v. Government of India, A.I.R. 2007 A.P. 102 (India) (*Per* G. Rohini, J.). The writ petition challenged the order of the respondent under section 5(2) of the Indian Telegraph Act, 1885 directing the interception of messages from the mobile phone of the petitioner. The court discussed the procedural propriety in the order of interception of communications framed under Rule 419-A of the Indian Telegraph Rules, 1951 framed pursuant to the safeguards given by the court in the *PUCL* case. The court examining the order discovered that it was lacking in the recording of reasons for the interception. The court also discovered that the review committee constituted under Rule 419-A(8) merely postponed the review of the order. Ultimately, the court held that these infirmities rendered the evidence inadmissible. Even here, the approach of the law enforcement agencies to not observe procedure is to be noted.

[96] Gulf, Colorado & Santa Fe Ry. Co. v. Ellis, 165 U.S. 150 (1891).

2. Absence of an effective injury discovery and redressal system

The problem of the non-adherence to procedure is compounded by the absence of an effective legal measure to discover the privacy harm, until the information is publicly distributed making the subject aware of the infraction. This seems necessary as a notification may cause the concealment of the information which is sought to be gathered. However, this problem is acute. I anticipate that the paucity of precedent challenging unwarranted intrusion can be attributed to the non-disclosure. The limited precedent at hand is in cases where an offence is alleged against a person and the information gathered through surveillance is presented in court. The limited empirical evidence suggests that unwarranted surveillance is a common occurrence. The *PUCL* case itself arose out of statistics of a study presented by the Central Bureau of Investigation which stated the high degree of warrantless eavesdropping on conversations of politicians.[97] A more recent case which touched media headlines was when the leader of a major political party complained that his phone was being tapped illegally.[98]

Even in the unlikely event that an ordinary person suspects that he is under electronic surveillance, his remedies are onerous to enforce. The Courts in their magnanimity may entertain (a) a writ proceeding under Article 226 or 32 of the Constitution of India for judicial review of the police action and for appropriate relief; (b) criminal action against the officers responsible for criminal trespass subject to other provisions of Code of Criminal Procedure, 1973; (c) damages in tort by filing a civil suit; and (d) appropriate compensation in a public law jurisdiction from the Court of judicial review under Article 226 or 32 of the Constitution.[99] These remedies may look attractive, however, they take substantial time, effort, money and lawyering to enforce.[100] Hence relying on litigation to cure privacy breaches will be ineffective.

---

[97] *Supra* note 48.

[98] Amar Singh v. Union of India, 2006 (2) S.C.A.L.E. 698 (India), at ¶ 2 (*Per* Y. K. Sabharwal, C.J.) ("we have asked certain questions from learned Solicitor General regarding the tapping of telephones under the authority of the Central Government for which too much time is sought to file further affidavits.").

[99] Sunkara Satyanarayana v. State of Andhra Pradesh, 2000 (1) A.L.D. (Cri.) 117 (India), at ¶ 65 (*Per* V. V. S. Rao, J.) (listing the different types of remedies available to a petitioner aggrieved by the police maintaining a history sheet for him on grounds of infringement of his right to privacy).

[100] ARUN MOHAN, JUSTICE, COURTS AND DELAY 1-42 (2009) (a modern classic on the causes and the solutions to delays clogging Indian courts); *see also* Marc Galanter, *Fifty Years On*, *in* SUPREME BUT NOT INFALLIBLE: ESSAYS IN HONOUR OF THE SUPREME COURT OF INDIA 57-65 (B. N. Kirpal et al. eds., 2004) (describing litigation in India as plagued by delays and as a game of a 'sunken cost auction').

B. A DEEPER CUT AT PRIVACY

The above defects are essentially inherent design defects in the provisions granting legal sanction for surveillance and may apply equally across all mediums of expression such as letters, telecommunications and internet communications. However, there are certain harms which accrue uniquely towards internet communications. This section analyses these unique harms which are not found present in other mediums and represent a higher degree of privacy harms.

The internet as an interactive medium provides persons with a wide range of applications suited to cater to every information need. These may be through the mediums of text or audio-video; however it is this broad range of applications it provides, which makes harms of interception, processing or disclosure cut much deeper. The cross synergies of these applications cause a deeper level of harm than with conventional telephone tapping. Moreover, a person accessing the internet often does so within the privacy of his own home and expects a reasonable level of privacy.[101] The communications when not with a human party are for the satisfaction of his or her own desires and curiosities. A person may divulge more information to a computer than to another person. This may be mundane and embarrassing as a music aficionado occasionally listening to bubble gum pop or as serious and damaging as a mentally ill person researching on alternate methods of treatment. Hence internet communications are inherently intimate and concern the core of the privacy of the person.

Internet communications are a reflection of a person's thought, intent and motive. To this effect the statement by John Battelle makes for chilling reading, "[l]ink by link, click by click, search is building possibly the most lasting, ponderous, and significant cultural artefact in the history of humankind: the database of intentions."[102] Hence, applying the same standards which have been set for telephone tapping would be a gross simplification of the problems which are posed by privacy harms in internet communications.

---

[101] Cyber Cafe in Gandhinagar, India, http://www.worldembassyinformation.com/india-cyber-cafe/cyber-cafe-in-gandhinagar.html (last visited July 5, 2010). This page shows cyber cafe listings in the city of Gandhinagar. Most of these establishments mention that they have dim lighting and offer the surfer complete privacy. In India, when visiting a cyber cafe to access the internet a person often finds a row of computers separated into separate cubicles providing privacy from other patrons glancing on the screen and gleaning information.

[102] John Battelle, The Database of Intentions (Nov. 13, 2003), http://battellemedia.com/archives/000063.php (last visited Jan. 4, 2010). *See also* Aloke Tikku & Gaurav Choudhury, *Database to fight terrorism will keep eye on you*, HINDUSTAN TIMES, Dec. 23, 2009, *available at* http://www.hindustantimes.com/News-Feed/india/Database-to-fight-terrorism-will-keep-eye-on-you/Article1-489540.aspx ("This means that rather than writing to more than 50 entities — government bodies such as the RBI and the Bureau of Immigration, and private firms like phone and airline companies — all that a security agency has to do is to feed your name into the system.").

C. ABSENCE OF WIDE DATA PROTECTION STANDARDS

1. Limited protection against private privacy risks

As highlighted above, the current privacy regime is designed to protect the civil liberties of citizens against the state. In such a set-up the protection which is afforded against private entities is the limited to the non performance of functions which they perform when under directions of state entities. Such an approach ignores the fundamental economics of the internet economy, where the state is a marginal player, and users' search habits are concentrated in a few online service providers. Here from the moment the basic access starts, a user usually logs onto a search engine or/and email service provider. Often both of these are operated by the same conglomerate, such as Yahoo!-Yahoo! mail,[103] Google-Gmail,[104] Bing-Hotmail.[105] This is not a slippery slope or an argument in anticipation. These companies' basic revenue model is devised on the basis of serving contextual advertisements to support their services. The use of such information can lead to a host of privacy harms. For e.g., the inventor of the internet itself has expressed concern that searching for books on cancer could result in increased health insurance premiums because companies can track consumer activity and then sell this information to the insurance industry.[106]

2. Non-recognition of the harm of information processing

The current privacy regime is also limited in the respect that it does not afford any protection against several harms which are incurred. These are most glaring with respect to the complete non-recognition of important harms caused by information processing. An unprecedented amount of personal data is available online and when aggregated a persons life becomes 'transparent' over time.[107] Increasing the level of privacy harm is the fact that the data is stored in vast private databases by a few conglomerates due to the concentrated nature of the online service industry.[108] However, when this data may be seen non-contextually it may lead to incorrect inferences being drawn, e.g. a person's search query logs may be entirely for the purposes of research and not a personal medical condition. What is most worrying is that a person whose data is being gathered

---

[103] Is your email privacy safe with Google's Gmail and Yahoo! Mail?, July 30, 2006, http://www.scooq.com/general/is-your-email-privacy-safe-with-googles-gmail-and-yahoo-mail/34/ (last visited July 5, 2010).

[104] BBC News, Google's Gmail Sparks Privacy Row, Apr. 5, 2004, http://news.bbc.co.uk/2/hi/3602745.stm (last visited July 5. 2010).

[105] Michael Arrington, Bing Comes to Hotmail, July 9, 2009, http://www.techcrunch.com/2009/07/09/bing-comes-to-hotmail/ (last visited Jan. 01, 2010).

[106] BBC News, Rory Cellan-Jones, Web Creator Rejects Net Tracking, Mar. 17, 2008, http://news.bbc.co.uk/2/hi/7299875.stm (last visited July 5, 2010).

[107] *See* Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433.

[108] *Id.* at 1456-1463.

does not have any notice causing a harm of exclusion. This is exclusion in information processing and not information gathering hence, there should not be any reason for such exclusion. Here, it is not out of place to heed the EU Law on Privacy which contains a basic prohibition against databases. Then there is also the probable harm of secondary use, where the information gathered will be used for purposes other than for which it was gathered. For a robust privacy regime more rules need to be prescribed to safeguard against harms to privacy which are uniquely occurring in internet communications.

V

CONCLUSION

Privacy advocates have to reconcile to the fact that their government has the right to intercept and monitor data in a specified set of circumstances. This is more pronounced given the current climate in which the sceptre of terrorism is haunting most countries. Once, an agreement on that premise is achieved; the circumstances for interception and monitoring as well as the safeguards to check the potential abuse are the next logical step. Without an effective design for incentives, checks or balances such procedures are cursory at best.

The provisions which have recently been made under the regulations are imperfect however they are not defective. They require refinement and substantiation and not whole scale repudiation. The best alternative keeping in view the procedural approach towards information gathering would be to mandate ex-ante ex-parte court orders. These orders may arise out of in-camera proceedings where a state counsel can provide particulars of the intrusion as well as the information which is sought. Such orders will cure the inherent defects in the system since they cleanly remove the inherent bias of the functionaries.

This will be a pragmatic and convenient compromise which will not mark a substantial shift in the present procedure driven approach. Such procedural safeguards are essential for internet communications since, as highlighted above, the level of the breach of privacy is higher than conventional invasions of privacy. At the same time the same safeguards which apply to section 69 should be applied to section 69B. Information aggregation and monitoring necessarily requires interception. Above and beyond this there is a clear causation of privacy harms which necessitate that the safeguards evolved by the *PUCL* Court under Article 21 for the 'right to privacy' are inserted in the section. To provide a robust protection of privacy rights regulations also have to be made regulating the role of private parties as to information processing.

The amendments without further refinement create Bentham's panopticon.[109] Encountered by issues of privacy on online communications, the legislature faces a tenuous task to take vital policy decisions. It finds itself in the position of a trapeze artist, where it cannot keep walking the tight rope, it has to take a call, tip over to totalitarian tendencies or embrace a newfound liberal conception. Obviously, only one of these choices affords a safety net to privacy.

[109] *See* JEREMY BENTHAM, PANOPTICON; OR, THE INSPECTION-HOUSE (1787), *reprinted in* THE WORKS OF JEREMY BENTHAM 37 (John Bowring ed., 1962) (an architectural design of a prison where the inmates' cells were designed in a manner whereby the Inspector of the prison could see and hear every inmate but it was impossible for an inmate to do so). *See also* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (1979).