January 2013 Volume 2 Issue 1
The Macrotheme Review
A multidisciplinary journal of global macro trends

Developing a constitutional boundary recognizing the protective and restrictive nature of anonymous speech in the cyber world

Adoksh Shastry
School of Law, Christ University, Bangalore, Karnataka, India, adoksh@gmail.com

Abstract

The development of the cyber world has enhanced the application of the constitutionally recognized rights of "neti-zens"to a wider spectrum than envisaged before. The right to freedom of speech and expression has always been under scrutiny by agencies of State in its application to the cyber world. With limited resources to trace the origin of such speech and with jurisdictional and political barriers aplenty, governments across the world have maintained a pseudo-consensual attitude towards permitting unrestricted free speech in the online world. With a lack of judicial or executive consensus in the international regime, an attempt to determine the constitutional validity of anonymous cyber speech and expression in the internet is crucial. There are however numerous constraints of law within which anonymous cyber speech can grow and develop. Privacy rights are at the heart of it and governments across the world face a tough balancing act between the rights of the individuals and the compelling state interest.The concern mounts with many nations adopting absolute restrictive measures hampering any sort of anonymous speech and expression in the online world. Unless the world draws upon itself, a uniform policy measuring the welfare of anonymous speech against its negative implications on state interest, arbitrariness and unlawful arrests and disclosures will continue. It is in the interest of the citizens of the world and the media that answers to key questions relating to the authority of the Government to seek disclosure of personally identifiable information, location and content information of anonymous users and posts from internet service providers, broadcasters and hosts is established. In doing so, an attempt can be made at developing a constitutional boundary recognizing the protective and restrictive nature of anonymous speech in the cyber world.

Keywords*: anonymous speech, the cyber world*

1. Introduction

The right to privacy has been enumerated upon by various courts across the world as being a basil right available to all.[1] The Freedom of speech and expression, provided for under Article 19(1) (a) of the Indian Constitution is an integral part of online communication and anonymity in expression has been held to be a vital tool for fostering healthy democratic participation. Any requirement to have collected the recognizable information of the users of a

[1] *Handyside v The United Kingdom* (App no 5493/72) ECHR 7 December 1976

website would most naturally curtail and deter free speech and expression which is against the tenants of International law requirements. [2]A legislative requirement mandating websites to collect and verify name and contact information of the users would seem in principle to violate their right to privacy. The collection of such personally identifiable information, a term commonly used to identify and specify information that would help in the identification of an individual; under legislative mandate without due notice and choice is a gross violation of the provisions of Article 12 of the Universal Declaration on Human Rights and other internationally and municipally recognized rights.[3]

This ideology of anonymity in expression has been upheld in the form of a general right to anonymity which is protected from arbitrary State interference. Restrictions upon the freedom of expression are thus limited to prescribed heads identified collectively and conclusively by Courts across the world. Thus any restriction upon such freedom must be at the first instance, provided by law, then pursue a legitimate aim and finally be necessary in the functionality of a democratic society.[4] The requirement to have disclosed by any website or internet service provider, an individual's identity or the identity of members of a questionable association, to the government heavily infringes upon privacy rights of the association or the individual and in turn could violate the right to freedom of association without state interference, guaranteed under the tenants of international law. Furthermore, any private nature of communication, developed and maintained through user settings and disclaimers clearly establishes the desire of the subject to maintain anonymity in association and the State is bound to respect such privacy and associational rights.[5]

Adding to privacy woes are several instances of the State action claiming historical location information of the users, knowing authoritatively that such historical location information is guarded by a reasonable expectation of privacy.[6] Courts and legal jurisprudence has been highly protective of location information and any State interference must be grounded on reasonable counts. The nature of information being historical, courts have however rejected such claims on grounds of violation of individual security and privacy.[7] To have the location information of an association or a group secured is of great importance for the privacy and security rights which forms the basis of anonymous free speech. Users of the net, maintain a reasonable expectation of privacy and this expectation of privacy is treated as being objectively

---

[2] *Compulsory Membership in an Association Prescribed by law for the Practice of Journalism,* Advisory Opinion OC-585, Inter-American Court of Human Rights Series A No 5 (13 November 1985) (IACHR)

[3] Lee Tien, *Innovation and the Information Environment: Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 Or. L. Rev. 117, 176 (1996).

[4] Catherine Crump, *Data Retention: Privacy, Anonymity, and Accountability Online*, Stanford Law Review Vol. 56 No. 1 191, 229 (2003).

[5] Diane Rowland, *Anonymity, Privacy and Cyberspace,* 15th Bileta Conference: Electronic Datasets and Access to Legal Information University of Warwick

[6] *Cream Holdings Ltd v Banerjee* [2004] UKHL 44; *United States v Karo* 468 US714 (1984); *Marques de Morais v Angola* AHRLR 3 (HRC 2005)

[7] Minjeong Kim, 'The Right To Anonymous Association In Cyberspace: US Legal Protection For Anonymity In Name, In Face, And In Action' (2010) 7:1 SCRIPTed

acceptable by the society at large.[8] It must be noted though that in almost every instance, European and American Courts have rejected the claim that location information captured by mobile phone towers, internet service providers and such like amounts to enforcement of the third party doctrine on the grounds of there being no voluntary transfer of information in cases of real time location information.[9]

2. Anonymity and Privacy: The causal link

The intensity of State's permissible interference with the privacy of individuals is an inverse relationship with the damage the interference is likely to cause.[10] The Indian Supreme Court ruled in *Malak Singh*[11] that, while exercising surveillance over reputed bad characters, habitual offenders, and potential offenders no encroachment upon the privacy must be allowed so as to offend such right guaranteed under Article 21 of the Indian Constitution, 1950. A subjective expectation of privacy thus exists with regard to what an individual seeks to preserve as private.[12]

Anonymous speech is exercised under the notion of thought of anonymity and governmental action cannot seek too abridge it. It has been accepted by Courts however that sometimes governments would have to act upon interests of public good and safety under reasonable suspicious grounds without having clear identifiable proof or causal link of evidentiary nature.[13] The Indian Law for example, through the Telegraph Act, 1885 allows for the government to take possession of any telegraph worked by a person and have it disclosed in situations warranting public safety and public order.[14] Such is also applicable explicitly to certain classes of people the government may identify.[15]

Anonymity in the cyber space is touted as being a direct coherent of privacy rights. This right to remain anonymous exemplifies the right to retain ones privacy rights. The two are directly related to the others existence. To remain anonymous would mean to accept and recognize the right to privacy.

3. Right to anonymous utilisation of cyber resources

Article 21 of the Constitution of India provides that "*No personal shall be deprived of his life or personal liberty except according to the procedure established by law"*. Further, Article 12 of the UDHR provides that "*No one shall be subjected to arbitrary interference with his privacy,*

---

[8] Jennifer B. Wieland, 'Note, Death of Publius: Toward a World without Anonymous Speech', (2001) 17 J.L. & Pol. 589 590–93

[9] *Segerstedt-Wiberg and others v Sweden* (App No 62332/00) ECHR 20 September 2005

[10] *Hatton v UK* (App No 36022/97) ECHR 8 July 2003

[11] *Malak Singh v State of Punjab* AIR 1981 SC760

[12] *Griswold v Connecticut 381 US 479 (1965)*

[13] *Terry v Ohio* 392 US 1 (1968)

[14] Indian Telegraph Act of 1885, Article 5(1)

[15] Indian Telegraph Act of 1885, Article 5(2)

family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[16]

The Indian Supreme Court has maintained that the right to privacy is a part of the 'right to life and personal liberty', which is a basic right enshrined under Article 21 of the Indian Constitution which cannot be abridged at any reasonable point.[17] The Court goes on to state that the first aspect of right to privacy would be breached when any advance is made towards a person's name and such like without his consent.[18] The requirement on users to provide '*Personal Identifiable Information*' *(hereinafter PII)* to websites or internet service providers, noticed in a large number of instances upon compulsion and without choice is a violation of their privacy. The US Supreme Court has held that the individual's interest and choice in disclosing personal matters and information is an integral part of '*Informational Privacy*'.[19] The ECtHR reiterates this legal notion, that the concept of private life extends to aspects relating to personal identity, such as a person's name[20] and that the right to informational privacy is of grave concern and one that should be protected from dissemination.[21] Furthermore The Council of Europe adopted the *Draft Declaration on Freedom of Communication on the Internet*, which provides that no State can compel or pass legislations which require the users of internet to in any way have their identity disclosed to the government or to the service provider.[22]

However, such a principle can never be construed as absolute and is subject to limitations placed under Article 29 (2) of the UDHR stating that '*in the exercise of such rights and freedoms, everyone shall be subject to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society."*[23]The positive obligations flowing from the fore part of Article 12 of the UDHR must strike balance with the aims mentioned under Article 29(2) of the UDHR and the due process, recognized by Constitutional instruments across the world must be adhered to.[24]

---

[16] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at: http://www.unhcr.org/refworld/docid/3ae6b3712c.html [accessed 21 August 2012]

[17] *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301

[18] *R. Rajagopal v State Of Tamil Nadu* 1995 AIR 264,

[19] *Whallen v Roe* 429 US 589 (1977)

[20] *Burghartz v Switzerland* (App No 16213/90) ECHR 22 February 1994; *Schüssel v Austria* (App No 42409/98) ECHR 21 February 2002

[21] *S and Marper v The United Kingdom* (App No 30562/04 and App No 30566/04) ECHR 4 December 2008

[22] Draft Declaration on Freedom of Communication on the Internet, CDMM Misc 18 of 2002, Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies

[23] *Supra* note 16 at Article 29(2)

[24] Powell and Rayner v The United Kingdom (App No 3/1989/163/219) ECHR 21 February 1990; *Lopez Ostra v Spain* (App No 16798/90) ECHR 9 December 1994

The US Supreme Court, in *Tehan v Shott* held that virtually every governmental action would seem to interfere with personal privacy to some degree; but the question was whether that violated a command of general constitutional right.[25] In view of this, *Katz v United States* made clear that although the Constitution affords protection against certain kinds of governmental intrusions into personal and private matters, there was no general constitutional right to privacy available to the citizens.[26] A notion of similar thought has been held by several Indian scholars, noting that while the Constitution expressly provides the Indian with the Right to Life, judicial interpretation fencing on activism claiming a right to privacy cannot be regarded as the soul of thought garnered by the forefathers drafting the Constitution. Such an argument dispenses the notion of spirit of law, in support of the text of law and would result over a period of time, in the manifestation of a legal system rigid and not flexible to the changing notions of law and society.

International law today however, remains blurred in the aspect of pinpointing an acceptable and authoritative line of privacy restriction for the people.[27] For instance the ACHR prohibits all restraints while the ECtHR allows restraints in certain limited circumstances under which the constitutionally recognized or derived right to privacy could be curtailed.[28] The ECJ in *Bavarian Lager v Commission* held that the mere collection of names by itself could not constitute an interference with the right to privacy of an individual. [29]US Courts and international scholars have repeatedly allowed Government access to names and other such information of persons on grounds that in the current society such did not comprise of personal information that warranted privacy protection.[30] Variance of such nature has sparked major difficulties amongst netizens in understanding the law as it is.

A rather new development in cyber research has been the *Safe Harbor Privacy Principle*- a generally accepted privacy norm in several nations notably the United States and the European Union.[31] The *Safe Harbor Privacy Principle* provides for 2 key requirements in view of any possible infringement of the right to privacy. Firstly, a *Notice* to be provided to the user stating the reasons for which disclosure and collection would be made of his information[32]and secondly,

---

[25] *Tehan v Shott* 382 US 406, 86 S Ct 459 (1966)

[26] *Katz v United States* 389 US 347

[27] Malcom N. Shaw, *International Law* (5th Ed., Cambridge University Press, UK 2003) 247

[28] *Case of Observer & Guardian v UK* (App No 13585/88) ECHR 26 November 1991

[29] *Bavarian Lager v Commission* (Case No T-194/04) ECJ 8 November 2007

[30] *State v Chryst* 793 P 2d 538, 542 (1990); *State v Faydo* 846 P 2d 539, 541 (1993); *Commonwealth v Duncan* 752 A 2d 404 (2000); Stephen E. Henderson, 'Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too' (2007) Pepperdine Law Review Vol. 34

[31] Commission Decision (EC) 2000/520 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the, Adequacy of the protection provided by the Safe Harbour Privacy Principles (notified under document number C(2000) 2441); Michael Erbschloe, John R. Vacca, *Net privacy: A guide to developing and implementing an ironclad e-business privacy plan* (McGraw-Hill Professional, 2001) 296

[32]Commission Decision (EC) 2000/520 Section 1; *Dendrite International v John Doe (No 3)* 342 NJ Super 134

the user must be given a *Choice* to disclose his personal information without being barred from accessing the net otherwise.[33]

4. The Right to Anonymous Cyber speech and expression

While the nature of anonymous cyber existence or utilization of the resources of the broadcaster or the Internet service provider may not seem in coherence with the theme of the paper, it is crucial towards establishing the link between anonymous existence in the online world and the right to freedom of speech and expression. Anonymity is an important method, perhaps the only reliable method, of protecting privacy on-line and has been recommended by both the OECD[34] and the Council of Europe, amongst many other entities of International prevalence.[35] In India, the Central Vigilance Commission mandated that no action should be taken on any anonymous/pseudonymous complaint, referring, that while it might be a loophole, such anonymous status warranted no compelling actions.[36] Further in *Srivastava v Northern Railways*,[37] the Allahabad High Court deemed a provision of the *Railways Rules* preventing anonymous speech, unconstitutional on the grounds of it violating Article 19(1) (a) of the Indian Constitution; the provision guaranteeing as a fundamental inalienable right of every citizen free speech and expression. The United States Supreme Court shares a similar view, and has been upholding the right to convey information anonymously and now applies strict scrutiny to governmental regulations impinging anonymous speech.[38]

The State's interference and ability to not permit anonymity would hinder and stop associations from providing privacy to its members within themselves and amongst members of the public.[39] In *Segerstedt-Wiberg & Ors v Sweden*[40] the ECtHR refused to grant access to Swedish police, personal information of users upholding the importance of privacy and anonymity in association. Moreover, *The freedom of expression on the Internet Declaration*, states that in order to enhance free expression of information and ideas, States should respect the will of users of the Internet not to have their identity disclosed.[41] Finally, in *Watchtower Bible & Tract Society v Village of Stratton* the ECtHR also held that anonymity helped shield unpopular

[33]Commission Decision (EC) 2000/520 Section 2

[34] Convention on the Organisation for Economic Co-operation and Development (OECD), Paris 1960-12-14

[35]Diane Rowland, 'Anonymity, Privacy and Cyberspace' (2000)15th BILETA Conference: Electronic Datasets And Access To Legal Information

[36] Central Vigilance Commissioner, Order No. 3(v)/99/2, On anonymous and pseudonymous complaints, 29th June 1999

[37] *Sudha Srivastava v Claims Commissioner, Northern Railways* 1 (1985) ACC 9

[38] Lee Tien, 'Innovation and the Information Environment: Who's Afraid of Anonymous Speech? McIntyre and the Internet' (1996)75 Or. L. Rev. 117, 176

[39]Jay Krasovec, 'Cyberspace: The Final Frontier, for Regulation'(1997) 31 Akron L. Rev. 101 138

[40]*Segerstedt-Wiberg and others v Sweden* (App No 62332/00) ECHR 20 September 2005

[41]Council of Europe Declaration, On freedom of communication on the Internet, Adopted by the Committee of Ministers of the Council of Europe on 28 May 2003

individuals and ideas from retaliation and suppression and regardless of the reason behind anonymity and the possibility of abuse, the value of free speech outweighed these concerns.[42]

It is clear that anonymous speech has played a key role throughout the course of human history and in founding of democratic nations.[43] Emphasizing the notion, the United States Supreme Court opined that speech on the internet received full First Amendment protection, including the right to speak anonymously.[44] The ability to speak freely is in most cases attributed to the ability to do so anonymously.[45] The right to remain anonymous is an integral part of the First Amendment principle of freedom of speech and expression.[46] In the case of *Talley v California*, it was pointed out that identification and fear of reprisal might deter perfectly peaceful discussions. [47] Furthermore, the European Parliament passed the *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*[48] which amplified the right to privacy of the users provided under the ECHR.[49]

5. The Right to unmask the anonymous

While the above understanding of Constitutional anonymity may remain judicially acceptable, several legal and scholarly forum believe that an absolute right to remain anonymous or to anonymous speech online cannot be expected or accorded.[50] The Indian Supreme Court taking into consideration the importance of restrictions in certain areas held that, if restrictions lead to prohibition only in a tailored area, such was not unreasonable.[51] The ECtHR echoes the finding and holds a non-availability of the right to anonymity in action when compared and

[42] *Watchtower Bible & Tract Society v Vill of Stratton* 536 US 150, 166–69 (2002); *Buckley v Am. Constitutional Law Found., Inc.,* 525 US 182, 204 (1999)

[43] *McIntyre v Ohio Elections Comm'n* 514 US 334, 341–43 (1995); *Talley v California* 362 US 60, 62 (1960); Jennifer B. Wieland, 'Note, Death of Publius: Toward a World without Anonymous Speech' (2001) 17 J.L.& Pol. 589 591-593

[44] *Reno v ACLU* 521 US 844, 870 (1997); *Doe I v Individuals (AutoAdmit.com)* 61 F Supp 2d 249, 253–54 (2008); *Doe No. 1 v. Cahill* 884 A 2d 451, 456 (2005)

[45] *Buckley v American Constitutional Law Foundation* 525 US 182 (1999)

[46] Emerson T I, 'Toward a general theory of the First Amendment', (1963) Yale Law J. 72:877 956

[47] *Talley v California* 362 US 60 (1960)

[48] Directive 95/46 (EC) of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 23/11/1995

[49] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

[50] *McIntyre v Ohio Elections Comm'n* 514 US 334, 357 (1995); *Talley v California* 362 US 60, 64–65(1960); *Doe I v Individuals* 561 F Supp 2d 249, 254 (2008); *Indep Newspapers Inc. v Brodie* 966 A 2d 432, 441(2009)

[51] *State of Gujarat v Mirzapur Moti Kureshi Kassab Jamat* (2005) 8 SCC 534

contrasted against state interest of disclosure.[52] In the *Greenpeace International case*, the Delhi High Court in India held that, there existed a fundamental difference between expression on Internet and expression in traditional media.[53] Legal scholars have agreed that while anonymity is a virtue of real world expression; the online world provided too many safeguards for anonymous speech[54] and such anonymous speech had to be restricted.[55]They agree that while Courts have identified the legal right to remain anonymous in several cases[56] such cannot be applied to the online world as the First amendment protection or freedom as I term it must be considered tailored narrowly.[57]

In addition to the compelling arguments bolstering governmental arguments, *The European Union Declaration on mass communication media and human rights*,[58] *The Council of Europe Declaration on Internet governance principles*,[59] *The Deauville Declaration on the Internet*[60] and *The Geneva Declaration on Internet Freedoms*[61] all concur upon an abridged right to anonymity when it comes to the concept of compelling state interest.

6. The Reasonability of a Restriction

Art 19(1) (a) of the Constitution of India provides for freedom of speech and expression and Article 13(2) of the Constitution holds that the *'State shall not make any law which takes away or abridges such rights'*. The Court's commitment to freedom of expression demands that suppression be not allowed unless absolute certainty of damages is anticipated and not be remote,

---

[52] *Case Of K.U. v Finland* (App No 2872/02) ECHR 2 December 2008 ; *Doe v 2TheMart.com Inc*. 140 F Supp 2d 1088, 1093 (2001); *Mobilisa, Inc. v Doe* 170 P 3d 712, 720 (2007); *Doe v Cahill* 884 A 2d 451 (2005)

[53] *Tata Sons Limited v Greenpeace International & Anr* 2011 (45) PTC 275 (Del)

[54]Al Teich, Mark S. Frankel, Rob Kling, Ya-ching Lee, 'Anonymous Communication Policies For The Internet: Results And Recommendations Of The AAAS Conference' (1999) The Information Society (TIS) Version 14/21

[55]Minjeong Kim, 'The Right To Anonymous Association In Cyberspace: US Legal Protection For Anonymity In Name, In Face, And In Action'(2010) SCRIPT-ed Vol. 7 No. 1

[56] Minjeong Kim, 'The Right To Anonymous Association In Cyberspace' (n 17)

[57]G du Pont, 'The Criminalization of True Anonymity in Cyberspace'(2010) 7 Michigan Telecommunications and Technology Law Review 191-216; M Froomkin, 'Regulation and Computing and Information Technology: Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases' (1996) 15 The Journal of Law and Commerce 395-507

[58] Council of Europe, Recommendation on mass communication media and human right, 582 (1970) Adopted on 23 January 1970

[59] Council of Europe, Declaration on Internet Governance Principles, Adopted by the Committee of Ministers of the Council of Europe on 21 September 2011

[60] G8 Summit, Deauville G8 Internet Declaration for Renewed Commitment For Freedom And Democracy, Adopted on May 27 2011

[61]Geneva Summit for Human Rights Tolerance and Democracy, Geneva Declaration on Internet Freedom, Adopted by the Human Rights Defenders and Civil Society Representatives on 2 March 2010

or conjectural or farfetched.[62] The Supreme Court has clearly identified in several cases, tests to determine reasonableness of any restriction and such is in concurrence with tests laid down by Courts across the world. The Supreme Court has primarily taken into consideration the *nature of the right infringed, purpose of the restriction, aim of the restriction and conditions prevalent at the point of time*.[63] In *Rangarajan v Jagjivan* the Court clarified that any restriction imposed upon the freedom of expression must be justified under the limitation clause (2) of Article 19 alone.[64] In *Gobind v State of M.P* the Supreme Court of India laid down that privacy claims can be breached when a compelling state interest was found to exist in the backdrop to State action.[65] The ECtHR in the case of *Hadjianastassiou v Greece* held that dissemination of military secrets cannot afford Article 10 protection and State interference with such dissemination shall be construed as being reasonable and within permissible limits. [66] Similarly the UDHR recognizes that such freedom of anonymous cyber speech cannot be absolute and is subject to restrictions laid down within it.[67] Courts across the world have reached a consensus on what these restrictions are and have laid down a 3 part test. Accordingly, any restriction on the freedom of expression has to *(i) be provided by law, (ii) pursue a legitimate aim* and *(iii) be necessary in a democratic society,* in order to be permissible.[68]

7. Anonymity of Cyber Personality through location information

The Law Commission of India in its 198th Report commented extensively on the importance of nondisclosure of location information, especially of witnesses or people who expressed matters credible of danger or worry.[69] In addition, Article 10(2) of the European Convention prevents the disclosure of information received by one in way of confidence. [70] This confidence is presented in the way of a reasonable expectation of privacy existing. The reasonable expectation of privacy was formulated in *Katz v United States* and it is said to exist when (i) *a person has exhibited an actual expectation of privacy* (ii) *the expectation is one*

[62] Law Commission of India, One Hundred And Seventy Ninth Report on, The Public Interest Disclosure and the Protection of Informers

[63] *Chintaman Rao v State of Madhya Pradhesh* (1950) SCR 759

[64] *Rangarajan v Jagjivan* (1989) 2 SCJ 128

[65] *Gobind v State of M.P* (1975) 2 SCC 148

[66] *Hadjianastassiou v Greece* (App No 12945/87) ECHR 23 November 1992

[67] *Supra* note 16 at Article 29(2)

[68] *The Sunday Times v United Kingdom* (App no 6538/74) ECHR 26 April 1979; *Compulsory Membership in an Association Prescribed by law for the Practice of Journalism* , Inter-American Court of Human Rights Series A No 5 (13 November 1985) (IACHR); *Media Rights Agenda and Others v Nigeria* (Comm No 105/93, 128/94, 130/94 and 152/96) African Commission on Human and People's Rights (1998) (ACHPR); *Womah Mukong v Cameroon* (Comm No 458/1991), U.N. Doc. CCPR/C/51/D/458/1991(1994) (HRC)

[69] Law Commission Of India, 198th Report on ,Identity Protection and Witness Protection, August 2006

[70] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended, Article 10(2)

that society is prepared to recognize as reasonable. That a person has exhibited an actual expectation of privacy is evident from his actions of maintaining private communications.[71]

Justice Lehnin maintains that it would be appalling if governments could obtain historical location information of users without due notice of any sort[72]. This reasonable expectancy of the users does not erode after the moment has passed.[73] Historical location disclosure would result in a breach of the '*Reasonable Expectation of Privacy'* that users possess.[74] Further, in *DeGregory*,[75] a United States Court concluded that state intrusion cannot be allowed because an overriding and compelling state interest did not exist in a case where (1) *there was no evidence showing any causal link* and (2) *the information being sought was historical*.

A government seeking location information about the users of the websites would be in clear breach of the principles of '*reasonable expectation of privacy'* that users possess with regards to personal information of the magnitude of their location.[76]

This argument is however subject to the fact that Indian and American Courts have accepted that the right to privacy may apply to people but not to places, thus excluding location wise privacy rights.[77] Clark in my opinion holds that the *Assumption of risk* doctrine squarely applies to historical location information because of the fact that it is a person's conscious decision to activate and operate an instrument and he '*assumes the risk*' that the service provider will turn over to law enforcement the location information that the user broadcasts as and when a requirement of compelling nature bestows such service provider.[78] In matters of the privacy of users as regards their location and its circumference with public sphere, Judge Sterns opined that the most that the historical location information might reveal is that a person might presently be found in the home but there is nothing about that disclosure that is to be deemed surveillance and a breach of privacy of the user.[79]

---

[71] *Griswold v Connecticut* 381 US 479 (1965)

[72] *In The Matter Of The Application of The United States Of America For An Order Directing A Provider Of Electronic Communication Service to disclose records to the Government* (n 66) at [611]

[73] *In re Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Information* 509 F Supp 2d 64, 74–75 (2007)

[74] *In The Matter Of The Application of The United States Of America For An Order Directing A Provider Of Electronic Communication Service to disclose records to the Government* 534 F Supp 2d 585

[75] *DeGregory v Attorney General* 368 US 825 (1966)

[76] *Kyllo v United States* 533 US 27, 121 S Ct 2038

[77] *Gobind* (n 30); *District Registrar and Collector, Hyderabad v Canara Bank* (2005) 1 SCC 496; *Katz* (n 6)

[78] M. Wesley Clark, 'Cell Phones as Tracking Devices' (n 72)

[79] Patrick T. Chamberlain, 'Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard' (2009) 66 WASH. & LEE L. REV. 1745 1788

8. Conclusion: Tackling New Media

The rise of the Information Technology era has given rise to problems of varied magnitudes in light of the protection and implementation of fundamental rights in the online world. Due to its deceptive nature and the inability to control the content posted onto it, the Internet remains a potent tool for cyber bullies or criminals to infringe upon the rights of the millions without fear or foul of the law. Marking this is the lack of political consensus in developed nations about a uniform cyber law module and the lack of infrastructural and technical knowledge in developing and underdeveloped nations.

The root of the problem lies in the source. The internet functions as an element of New Media; as a source of information which should not to its widest possible limits be abridged. Cyber speech is merged with the constitutionally available right of free speech. No difference can be pointed out in an attempt to stifle the exercise of one's right. New Media requires a better understanding of the Cyber world, in order to better exercise the right to speech and expression. Understandably, the governments of the world are deterred by the concept of unbridled free speech and expression in a medium connecting over a billion people and the author is against such notion too. Unbridled free speech is a myth, a tale conjured by those unwilling to submit to the supremacy and rule of law. Instances of necessity, outgrowing personal limits require the State to take informed action in accordance with the law. The due process clause is crucial towards embodying a structure of recognition and restriction of rights.

Anonymous free speech has been of legal dispute since before the development of New media. The *N.Y Times* case and the *Karo-Katz* judgments are an exemplification of the view of the Court in protecting anonymous free speech. The Indian and European Courts along with the decisions of several African, Asian and South American Courts and Tribunals point in favor of permitting anonymous free speech. However, no Court has ever plainly provided for unrestricted free speech-anonymous or not. The existence of reasonable restrictions is crucial towards the usage of fundamental right of speech and expression in the online world.

Today, with the sluggish speed of cyber legislative developments, criminals still enjoy a large degree of freedom. Anonymous speech is restricted heavily in some nations while others glorify it as a part of the legal system. This lack of political consensus has given rise to trans-boundary cyber crime issues which frail from any impetus in the real world due to jurisdictional and personality bars. Anonymous free speech is a recognized right, but one subject to restrictions. Reasonable restrictions in accordance with the due process of the law enable a control mechanism over the anonymity of the individual in the cyber world. For now, unmasking the Internet remains a Governmental policy measure, implemented in testing times for the benefit and welfare of the nation as a whole; but one that also gives scope for abuse and violation of the sacred right to freedom of speech and expression of the individual.