IS THE NATIONAL PHARMACEUTICAL POLICY, 2012 REALLY CHEERING THE PHARMA?

*Dipika Jain**

The National Pharmaceutical Policy was approved by the Cabinet and notified in 2012. Based on this policy, a new Drugs Price Control Order was notified in May, 2013. As a result, several drugs will come within the ambit of price control under the National list of Essential Medicines (NLEM). The primary purpose of NLEM is to facilitate the rational use of medicines which will allow for cost effective, safe and drugs with efficacy. This paper critically evaluates the provision on exclusion of patented drugs in the recent National Pharmaceutical Policy, 2012 from the Drug Pricing Policy for five years. The policy states "Drugs patented under the Indian Patents Act, 1970 and which have been made as a result of indigenous products or process have been exempted from price control for a period of five years." Further, a formulation involving a new delivery system developed through indigenous R&D would be eligible for exemption from price control for a period of five years from the date of its market approval in India. While this exclusion may have been designed keeping the opportunity for innovation for pharmaceutical companies, however, given the critical situation of HIV/AIDSs medication, cancer drugs, tuberculosis etc., it is pertinent to have these drugs under price control well before the prescribed period of five years. This paper argues that this provision of the NLEM, 2012 contravenes the main objective of this policy and in turn violates the Constitutional right to life and health of millions of people who need these patented lifesaving drugs, especially the people living with HIV/AIDS (PHLAs).

Introduction

Access to essential drugs is a pressing concern in India today. This concern was in part exacerbated by India's transition from a process patent regime to a product patent one in 2005.[1] Essential drugs like the antiretroviral ('ARV') medicines for HIV/AIDS treatment and anti-cancer drugs are likely to become unaffordable due to implementation of the product patent in the Indian Patent Act, 2005.[2] The changes are likely to result in grave shortage in supplying ARV drugs to people in poor countries[3] and may encourage pharmaceutical company to prioritize revenues above the genuine needs of public health.[4] There are a few flexibilities available within Trade Related Intellectual

* Dipika Jain is Assistant Professor of Law and Executive Director of the Centre for Health Law, Ethics and Technology at the Jindal Global Law School (Delhi, India). I would like thank my colleagues Prof. Rehan Abeyratne and Prof. Nupur Chowdhury for reading over my draft and providing helpful comments.I would like to thank Kavya K. and Parvati P. for their able research assistance.

[2] Ministry of Health and Family Welfare Government of India, REPORT OF NATIONAL COMMISSION ON MACRO ECONOMICS AND HEALTH (2005), page 6, available at http://www.who.int/macrohealth/action/Report%20of%20the%20National%20Commission.pdf

[3] Sorcha O'Carroll, *Importing Indian Generic Drugs Following TRIPS: Case Studies from Zambia and Kenya*, available at http://www.mcmillan.ca/Files/SOCarroll_ImportingIndianGenericDrugs.pdf

[4] *See* Cecilia Oh, *TRIPS and Pharmaceuticals: A Case of Corporate Profits over Public Health*, THIRD WORLD NETWORK, Aug.-Sept. 2000, available at www.twnside.org.sg/title/twr120a.htm.

Property Rights Agreement under the WTO regime (TRIPS). Beyond the patent regulations and other available flexibilities in the national and international legislations, drug pricing is another available ex post remedy to regulate access essential drugs by ensuring affordability.

Drug pricing is crucial towards making drugs affordable to ordinary citizens. Many price control policies have been introduced in India from time to time.[5] These policies were driven by the twin objective of controlling the prices of essential (and later, bulk) drugs but also sought to simultaneously ensure the availability of these drugs and to meet the requirements of the industry for cost effective production, invention and capacity building.[6]

However, post-liberalization in 2002, a new pricing policy for pharmaceuticals was presented which sought to liberalize the prices control further.[7] This 2002 Policy was challenged in the High Court at Karnataka and the Court issued a stay on the implementation of the policy on 12.11.2002.[8] The Government challenged this order in the Supreme Court. The Apex Court vacated the stay but directed the Government to devise suitable criteria to make sure that essential, lifesaving drugs remained under price control.[9] It also directed the Government to review these drugs until May, 2003.[10] Therefore, the Drug Policy of 1994 remained in effect.

The All India Drug Action Network (AIDAN), along with other NGOs, filed a PIL in 2003 before the Supreme Court, challenging the Government's drug pricing policy.[11] The main plea of this public interest litigation was to ensure that the prices of essential drugs remain within the reach of

---

[5] *Id.* In India, the first drug pricing policy was implemented in 1963 under the Defence of India Act. The other are-the Drugs (Prices Control) Order of 1966, the Drugs (Prices Control) Order of 1970, issued under the "Essential Commodities Act 1955 by declaring drugs to be essential commodities under the EC Act, 1955; the Drugs (Prices Control) Order of 1979 and Drugs (Prices Control) Order, 1987 were issued following the declaration of Drug Policy, 1978 and Drug Policy 1986.

[6] *Supra* note 4.

[7] *Supra* note 4.

[8] NATIONAL PHARMACEUTICALS PRICING POLICY, 2012 (7th December, 2012), available at http://www.pharmaceuticals.gov.in/NPPP2012.pdf

[9] *Supra* note 8.

[10] *Supra* note 8.

[11] S Srinivasan, A network for the rational and ethical use of drugs, Indian Journal of Medical Ethics, 11 January 2013, available at http://www.issuesinmedicalethics.org/121di013.html

See also *Medicine Prices shouldn't rise: Supreme Court*, THE ECONOMIC TIMES, Nov 17, 2011 available at http://articles.economictimes.indiatimes.com/2011-11-17/news/30410046_1_drug-pricing-policy-essential-medicines-prices-control

the common man.[12] The Government set up a Committee in November 2004 to investigate the options and alternatives of price control and related issues and accordingly make suggestions to ensure the availability of essential, lifesaving drugs at affordable prices.[13] This Committee offered its suggestions in September 2005.[14]

In the meanwhile, the Ministry of Health and Family Welfare revised the list of drugs and notified the new National List of Essential Medicine (NLEM), 2011.[15] Due to concerns raised by various stakeholders and difference between Ministries, the 2011 list was replaced by the new NLEM, 2012. This list consists of "those medicines that satisfy the priority healthcare needs of majority of the population."[16]

The National Pharmaceutical Policy, 2012

The National Pharmaceutical Policy was approved by the Cabinet and notified in 2012.[17] Based on this policy, a new Drugs Price Control Order was notified in May, 2013. A list of several drugs will come within the ambit of price control called the National list of Essential Medicines (NLEM). The primary purpose of NLEM is to facilitate the rational use of medicines which will allow for cost effective, safe and drugs with efficacy. [18] This paper critically evaluates the provision on exclusion of patented drugs in the recent National Pharmaceutical Policy, 2012 from the Drug Pricing Policy for five years. The policy states "*Drugs patented under the Indian Patents Act, 1970 and which have been made as a result of indigenous products or process have been exempted from price control for a period of five years.*" Further, a formulation involving a new delivery system developed through indigenous R&D would be eligible for exemption from price control for a period of 5 years from the date of

[12] *Medicine Prices shouldn't rise: Supreme Court*, IBNLIVE, 18 November 2011, available at http://ibnlive.in.com/news/medicine-prices-shouldnt-rise-supreme-court/203413-17.html

[13] *Id.*

[14] *Supra* note 12.

[15] *Supra* note 12.

[16] NATIONAL LIST OF ESSENTIAL MEDICINES OF INDIA 2011, available at http://mohfw.nic.in/WriteReadData/l892s/4767463099list.pdf

[17] *Government notifies new drug pricing policy, cheaper drugs on way*, FINANCIAL EXPRESS, 13 December, 2012, available at http://www.financialexpress.com/news/government-notifies-new-drug-pricing-policy-cheaper-drugs-on-way/1044845

[18] *Supra* note 17.

its market approval in India. While this exclusion may have been designed keeping the opportunity for innovation for pharmaceutical companies, however, given the critical situation of HIV/AIDSs medication, cancer drugs, tuberculosis etc., it is pertinent to have these drugs under price control much before five years. Exception of 5 years will make accessibility to drugs extremely difficult.

This paper argues that this provision of the NLEM, 2012 contravenes the main objective of this policy and in turn violates the Constitutional right to life and health of millions of people who need these patented lifesaving drugs, especially the people living with HIV/AIDS (PHLAs). While most of the Drug Pricing Policies in the past have been implemented in light of various objectives, the 2012 National Pharmaceutical Policy is aimed mainly at making drugs affordable. The main objective of the 2012 policy is to put in place a regulatory framework to ensure the availability of essential drugs listed in the NLEM at affordable prices.[19] Other measures for encouraging the growth of the Pharmaceutical Industry and the development of new medicines, etc. will be adopted by the Government at a later time.[20]

It is apparent form this provision that the Government has once again failed to address the most pressing concerns relating to patented drugs in India. Patented drugs, especially the essential and lifesaving drugs must be bought under price control. Many essential and lifesaving and ARV drugs introduced in India after 2005 will be patent protected.[21] Although patents are provisional and will eventually expire, since ARV is a relatively new invention and will take some time before these come off patent, many people living with HIV/AIDS will not be able to afford these drugs and may die for lack of access to these antiretroviral drugs.[22] People living with HIV/AIDS are likely to develop resistance to first generation drugs and will need second-generation drugs soon. The second and third generation drugs are mostly patented.[23] The civil society has been filing patent

---

[19] *Supra* note 17*; supra* note 2.

[20] *Supra* note 2.

[21] Harriet Gliddon, *The end of the line for affordable HIV drugs?* , available at http://aglobalvillage.org/journal/issue3/global_health_and_development/hiv-drugs/ and Rachel Rizal, *Patents versus people: The battle over genericantiretroviraldrugs in India,* 8 INT. J. HEALTH ETHICS & POL'Y 1, 15 (2008) available at *http://ase.tufts.edu/tuftscope*

[22] Edwin Cameron, *Patents and public health: principle, politics and paradox*, 19 October, 2004 available at http://www.law.ed.ac.uk/ahrc/script-ed/docs/cameron.asp#Causes

[23] WHO HIV DRUG RESISTANCE REPORT, 2012 available at http://www.who.int/hiv/pub/drugresistance/report2012/en/index.html; Eben Harrel, *New Study Raises Concerns About HIV-Drug Resistance*, TIME, 14 January 2010, available at http://www.time.com/time/health/article/0,8599,1953718,00.html

oppositions[24] to block patenting of these lifesaving drugs. While some of these patent opposition petitions were successful[25] others were not. [26]

In this scenario, if these patented drugs remain outside price control mechanism, it defeats the purpose of this policy. It is pertinent to note that effective treatment for PLHA involves use of multiple drugs in a process called "combination therapy." The use of multiple drug therapies is mostly considered better because it decreases the chance of developing drug-resistant strains of HIV by cancelling out mutations against other drugs.[27] Lack of access to one drug in a combination therapy can impedes effective treatment. According to Médecins Sans Frontières (MSF), the fixed-dose combination of d4T/3TC/NVP, a generic triple combination therapy costs 26 times less than using the originator's triple therapy.[28] Though NVP and d4T were off-patent, Glaxo-Smith-Kline's (GSK) patent on the ARV 3TC obstructed the availability of this drug.[29]

Further, the lack of availability of one patented drug in multiple combination therapy can encourage the government to roll out drugs that may exclude the patented component. For instance, the ARV 3TC was under patent protection, hence inaccessible in China. Therefore, the government advocated a therapeutic regime which excluded 3TC.[30]

---

[24] On 30 March 2006, the Manipur Network of Positive People (MNP), and the Lawyers' Collective HIV/AIDS Unit filed an application opposing the patent application filed in the Kolkata patent office by Glaxo Group Limited for Combivir, a fixed-dose combination of two AIDS drugs (zidovudine/lamivudine, or AZT/3TC), Brazilian Interdisciplinary AIDS Association (ABIA) and the Indian NGO SAHARA submitted a joint pre-grant opposition to the patent application of Tenofovir Disoproxil Fumarate in India, The Indian Network for People Living with HIV/AIDS (INP+) and the Delhi Network of Positive People filed an opposition to the patent application on the AIDS drug tenofovir disoproxil fumarate (TDF), see also, Sangeeta Shashikant, *Indian opposition to drug patents*, TWN INFO SERVICE ON HEALTH ISSUES, 23 May, 2006, available at http://www.twnside.org.sg/title2/health.info/twninfohealth018.htm

[25] India's first post grant opposition was successful, the Intellectual Property Appellate Board (IPAB) has revoked the patent on Roche's pegylated interferon alfa-2a in 2012, see http://www.thehindubusinessline.com/companies/patent-on-roche-hepatitis-c-drug-revoked/article4057999.ece?homepage=true&css=print#> and the Cipla's patent opposition application was successfully against Pfizer in 2012, see http://www.business-standard.com/article/companies/cipla-wins-patent-opposition-against-pfizer-s-cancer-drug-112100400199_1.html

[26] See also Geeta Anand, *Drug Makers Decry Indian Patent Law*, WALL STREET JOURNAL, February 11, 2010, available at http://online.wsj.com/article/SB10001424052748703455804575057621354459804.html

[27] King JR, Acosta EP, Chadwick E, et al, *Evaluation of multiple drug therapy in human immunodeficiency virus-infected pediatric patients*, 22 PEDIATR. INFECT. DIS. J. 3 (2003), available at http://www.ncbi.nlm.nih.gov/pubmed/12634585

[28] Cheri Grace, *A Briefing Paper for DFID: Update on China and India and Access to Medicines*, DFID HEALTH RESOURCE CENTRE, 19 (November, 2005).

[29] *Ibid.*, at 4

[30] *Supra* note 29, at 18

It is clear that access to proper antiretroviral treatment is limited due to the high costs associated with patented ARV drugs. With new waves of ARV drugs being produced to combat resistance, access to proper treatment will only worsen as these new drugs are subject to patent protection. Price control on patented drugs is essential because a medicine market is not a perfect market and lack of price control will lead to exorbitant pricing.[31] Increasingly, drugs in India are purchased through private, out of the packet expenditure (79% according to a WHO study)[32]. Exemption form price control for a period of five years is extremely unreasonable and is likely to adversely impact the availability of lifesaving drugs. Even provisions like compulsory licensing, allow for only a three year lock-in period which is under considerable criticism. One of the main reasons for the three year lock-in period for compulsory licensing and the 5 year exemption for price control is imposed mainly because there is an argument that patents represent one of the most important incentives for commercial enterprises to undertake research and development.[33] The proponents of TRIPS argued that the 2005 amendments will encourage foreign investment, transfer of technology and increase investment in research and development of neglected diseases. However, the evidence has shown otherwise. There is also evidence to show that a strong patent regime does not necessarily guarantee increased investment in Research and Development (R&D).[34] Overall, evidence shows that the implementation of stringent patent rights in developing countries has had a negative impact on access to treatment, especially for PLHAs.[35] These time lags may result in prolonged delay in accessing essential medications.

Constitutional Right to Health

The exemption on patented drugs under the NPP is in violation of the right to life under Constitution of India. By recognizing that the fundamental right to life in Article 21 of the

---

[31] REPORT OF THE COMMITTEE ON PRICE NEGOTIATIONS FOR PATENTED DRUGS, Page 1 (Para1.1), available at http://www.elsevierbi.com/~/media/Supporting%20Documents/Pharmasia%20News/2012/August/India%20Patent%20Drug%20Pricing%20Report.pdf

[32] *Id.*

[33] *See, e.g.*, Jorge A. Goldstein & Elina Golod, *Human Gene Patents*, 77 ACAD. MED 12, 1315, 1323–24 (2002).

[34] *Why today's R&D model doesn't work for the needs of developing countries*, MÉDECINS SANS FRONTIÈRES (May, 2012) available at http://www.msfaccess.org/sites/default/files/MSF_assets/Innovation/Docs/MedInno_Briefing_GlobalConventionRD_ENG_2012Update.pdf

[35] Dipika Jain and Rachel Stephens, *The Struggle for Access to Treatment for HIV/AIDS in India*, COMBAT LAW PUBLICATION, 113 – 114 (2008).

Constitution emphasizes the value of human dignity, the Supreme Court began to address the importance of health as a fundamental right for Indian citizens. In addition to Article 47, the right to health also has its genesis in Articles 38[36], 39(e)[37], 41[38] and 48A[39] of the Directive Principles. In a series of cases, the Supreme Court[40] has addressed the issue of healthcare as a fundamental right and has imposed an obligation upon the state to take all steps to create conditions necessary for good health, including facilities for basic curative and preventive health service. Lack of access to essential and lifesaving drugs constitutes a violation of their right to the highest attainable standard of health and therefore, the right to life.[41] Courts around the world have relied on the rights to life and health to ensure their respective Governments provide HIV/AIDS treatment to those in need.[42] In 2001, the Supreme Court of El Salvador in *Jorge Odir Miranda Cortez v. Director of the Salvadoran Institute of Social Security*[43] held that the El Savadorian Government must provide ARV therapy and other medications that prevent the death and improve the quality of life of persons

---

[36] State to secure a social order for the promotion of welfare of the people.- (1) The State shall strive to promote the welfare of the people by securing and protecting as effectively as it may a social order in which justice, social, economic and political, shall inform all the institutions of the national life. (2) The state shall, in particular, strive to minimise the inequalities in income, and endeavour to eliminate inequalities in status, facilities and opportunities, not only amongst individuals but also amongst groups of people residing in different areas or engaged in different vocations

[37] Certain principles of policy to be followed by the State: - The State shall, in particular, direct its policy towards securing. (e) that the health and strength of workers, men and women, and the tender age of children are not abused and that citizens are not forced by economic necessity to enter avocations unsuited to their age or strength;

[38] Right to work, to education and to public assistance in certain cases.- The state shall, within the limits of its economic capacity and development, make effective provision for securing the right to work, to education and to public assistance in cases of unemployment, old age, sickness and disablement, and in other cases of undeserved want

[39] Article 48A: Protection and improvement of environment and safeguarding of forests and wild life - The State shall endeavour to protect and improve the environment and to safeguard the forests and wild life of the country

[40] In *Consumer Education and Research Centres & Others.* v. *Union of India,* (1995) 3 SCC 42, the Supreme Court held that the right to health and medical aid to protect health is a fundamental right and that health implies more than an absence of sickness. The Supreme Court in another case, *State of Punjab and Others* v. *Mohinder Singh Chawala*, (1997) 2 SCC 83, reiterated that that the right to health is integral to the right to life and that the Government has a constitutional obligation to provide healthcare facilities.

[41] Hans V Hogerzeil, *Essential medicines and human rights: what can they learn from each other?*, 84(3) BULLETIN OF THE WORLD HEALTH ORGANIZATION, 371-375 (2006), available at http://www.who.int/bulletin/volumes/84/5/371.pdf

[42] See *Diego Serna Gómez* v. *Hospital Universitario del Valle*; *XXX v. Instituto de Seguros Sociales (ISS)*; *Asociación Benghalensis et al. vs. Ministerio de Salud y Acción Social;*

[43] *Mr. Jorge Odir Miranda Cortez v. la Directora del instituto Salvadoreño del Seguro Social*, Constitutional Court of El Salvador, File n°348-99 (4 April 2001).

living with HIV/AIDS.[44] Similarly, In 1995, in *XXX v. Instituto de Seguros Sociales (ISS)*[45], the Columbian Constitutional Court, in 1997, in *William García Álvarez v. Caja Costarricense de Seguro Social*[46] and in 2000, the Argentinean Supreme Court in *Asociación Benghalensis et al. vs. Ministerio de Salud y Acción Social*[47], the respective Supreme Courts ruled that ARVs must be provided through the Government's social security scheme and public hospitals. The court based its decision on the importance of the rights to life and health. Moreover, a Colombian appellate court recently held that the Ministry of Health violated the right to health by not having Abbott comply with the reference price for Kaletra. Resultantly, the Ministry imposed this requirement and the price of Kaletra was reduced by 70 percent.[48] Therefore, this policy of the government is violating the right to health and right to life of people living with HIV/AIDS by not bringing affordable patented drugs within the Price Control Policy of the government, which is being implemented with the main aim of providing access to affordable lifesaving drugs.

Further in the on-going litigation in the Supreme Court, In *All India Drug Action Network (AIDAN) v. Union of India*[49], the Indian Supreme Court opined during the hearing in July 2012 that the government must make every effort to provide access to lifesaving drugs to the citizens. Hence, the patent exemption for 5 years must be reconsidered and the patented drugs must be brought within the price control policy of the government before the actual notification of the Price drug Order happens.

Conclusion

It is imperative for the government to reconsider the exemption clause for patented drugs under the NPP, 2012 and allow for exemption of price control of patented drugs only for a very short duration, if at all, and establish a robust mechanism by which prices can be fixed and these drugs can be made accessible to save lives of several people living with HIV/AIDSs. The TRIPS Agreement itself contains flexible mechanisms for balancing access to treatment with the

---

[44] *Mr. Jorge Odir Miranda Cortez v. la Directora del instituto Salvadoreño del Seguro Social*, Constitutional Court of El Salvador, File n°348-99 (4 April 2001).

[45] Sentencia T-271/95, Exp. 62714, of Seventh Court of Revision of the Constitutional Court (June 23, 1995).

[46] *Mr. William Garcia Alvarez v. Caja Costarricense de Seguro Social*, Constitutional court of Costa Rica, File 5778-V-97, 23 September 1997.

[47] *Asociación Benghalensis et al. v. Ministerio de Salud y Acción Social*, Supreme Court of Justice of Argentina, Fallos 323:1339, 1 June 2000.

[48] Public Citizen, Access Victories and Global Kaletra Campaign, available at http://www.citizen.org/Page.aspx?pid=5798

[49] Writ Petition (civil) no(s). 423 of 2003.

preservation of intellectual property rights, such as compulsory licensing, parallel importation and patent opposition procedures. However, these instruments will inherently be limited in enhancing access to treatment because the successful implementation of each depends on several legal, administrative and political factors. The litigation with Novartis[50] and the unsuccessful patent oppositions[51] are some examples of such limitations that further delay or deny access to affordable lifesaving drugs. . The Indian Government must reconsider this and deliberate on whether the best interests of the country is allowing for an inclusive price control policy or struggle with other restrictive or limiting provisions available.

---

[50] Novartis AG v. Union of India (2007) 4 MLJ 1153.

[51] *Supra* note 32.

RENEWABLE ENERGY AND THE WTO: THE LIMITS OF GOVERNMENT INTERVENTION

James J. Nedumpara*

This paper examines the role of the government in designing and supporting renewable energy programs and the compatibility of such interventions with various covered agreements of the World Trade Organisation ('WTO'). The WTO treaty does not provide a special framework for renewable energy and a number of programs are susceptible to WTO challenges and domestic trade contingency measures. Of particular interest to developing countries such as India will be the availability of necessary policy space in fostering various renewable energy programs. This paper discusses the current treaty provisions of the WTO, especially the Agreement on Subsidies and Countervailing Measures ('SCM Agreement') and the Agreement on Trade Related Investment Measures ('TRIMs Agreement') and examines the extent of space in policy making available to various WTO Members across varying levels of development. In short, the paper seeks to examine the limits of WTO-consistent government intervention in the field of renewable energy.

Introduction

The world's leading economies have been pledging support for developing alternative and cleaner forms of energy, especially in the new millennium. According to the International Energy Agency ('IEA'), fossil fuels (oil, coal, and natural gas) will remain the dominant source of energy for the immediate future, but their share in the energy mix is bound to progressively decline in the future. IEA estimates that renewable energy demand may increase in 2035 by an amount ranging from 14 percent to 27 percent.

Recent years have witnessed massive growth in investment in the renewable energy sector in some of the developed countries. In the United States, renewable energy constitutes almost twelve percent of the total energy capacity. Focus on clean energy also means that the scope of governmental intervention has risen significantly. President Obama's FY 2013 budget, which seeks to support the continued manufacture, development and deployment of clean energy technologies, includes $5 billion in tax credits.[1] Similar measures have been adopted by various countries,

* Assistant Dean and Executive Director, Center for International Trade and Economic Laws, Jindal Global Law School, NCR of Delhi. India. The author may be reached at: jnedumpara@jgu.edu.in.

[1] *The blueprint for A Secure Energy Future: Progress Report* (2012) *available at* http://www.whitehouse.gov/sites/default/files/emailfiles/the_blueprint_for_a_secure_energy_future_oneyear_progress_report.pdf

including the EU and Japan.[2]

The BRICS group (consisting of Brazil, Russia, India, China and South Africa) has already emerged as a major consumer of energy resources. China has recently overtaken the United States as the largest consumer of energy and energy-related resources. However, China has initiated several programs for generation of renewable energy. China is the leading installer of wind turbines and solar systems in the world.[3] It is also the leading hydropower producer. Likewise, India is one of the first countries in the world to establish a dedicated Ministry of Non-conventional Energy Resources. Since its launch in 2010, the Jawaharlal Nehru National Solar Mission (JNNSM) has been a key feature of the National Action Plan on Climate Change.[4] India has set a target of scaling up to at least ten percent of all new capacity in the field of renewable energy. Brazil, another prominent BRICS country, has been supporting the Program of Incentives for Alternative Electricity Resources (PROFINA) since 2002. Brazil is also the second largest producer (after the United States) of fuel ethanol and the world's largest exporter of ethanol.

There are other developed countries that have initiated massive programs for promoting renewable energy. Germany is the pioneer, and perhaps, the most successful country in the world in introducing a Feed-in-Tariff ('FiT') scheme. A FiT Scheme provides a guaranteed tariff to electricity produced from renewable energy sources.[5] The German FiT law, which was introduced in 1990, required utilities to provide renewable energy generators grid access and also purchase the energy produced. The German FiT program, which has since been revised, imposes an obligation on private distribution and transmission system operators to purchase and share the costs of paying the statute mandated tariff to the renewable energy producers. Germany's success in

---

[2] Arunabha Ghosh and Himani Gangania, *Governing Clean Energy Subsidies: What, Why and How Legal*, ICTSD Global Platform on Climate Change, Trade and Sustainable Energy, 29-36, (August 2012), *available at* http://ictsd.org/downloads/2012/09/governing-clean-energy-subsidies-what-why-and-how-legal.pdf

[3] Renewable Energy Policy Network, *Renewables 2011 Global Status Report*, (September 2010).

[4] The JNNSM seeks to install 22 GW of solar power (grid and off-grid) using both PV and concentrated solar power technologies by 2022.

[5] A FiT is essentially a purchasing guarantee. This is generally done by the government through electricity utilities (may be either private or public bodies) on the directions of the government. In the case of the FiT scheme run by the Ontario Power Authority, a body that was created by provincial government statute in 2004, the program allows both large-scale (above ten kilowatts) and small scale (less than ten kilowatts) private energy producers with qualifying renewable energy fuel sources (including solar photovoltaic cells, water, wind and bioenergy production systems) to resell generated energy back onto the Ontario electricity grid at a fixed price for a twenty-year period.

introducing the FiT program has inspired several countries, including Canada.[6] As of now, nearly sixty-three countries have started offering FiTs.[7] The Canadian province of Ontario introduced the FiT and the micro FiT program, which is now in the midst of a WTO challenge.[8] The Preamble of the Green Energy Act passed by the Canadian government provides that the legislation strives towards "cleaner sources of energy" as well as the promotion of both, renewable energy projects and a "green economy".

The focus on clean and renewable forms of energy is indeed welcomed by all. However, the development of renewable energy programs has also raised significant concerns. The subsidies for renewable energy were about US $ 66 billion in 2010 alone. In the new policy scenario, subsidies to renewable energy will reach US$250 billion in 2035. Renewable energy support schemes are generally in the form of targets, mandatory quotas, price support (e.g. FiTs), tax incentives such as Production Tax Credits (PTC), Renewable Portfolio Standards (RPS), loans, grants, and various types of incentive schemes.[9]

The subsidies and other government support assume various forms. In China, the grants to Chinese wind turbine manufacturers were conditioned on use of key parts and components made in China rather than purchasing imports.[10] In Canada, the Ontario FiT program requires the solar and wind facilities to meet domestic content requirements, i.e., 60 percent and 50 percent for solar and wind projects respectively. India requires solar power developers, or their successors in contract, to purchase and use solar cells and solar modules of domestic origin in order to participate in the JNNSM and to enter into and maintain power purchase agreements under the JNNSM or with the National Thermal Power Company Vidyut Vyapar Nigam Limited. As a result, solar power developers, or their successors in contract, receive certain benefits and advantages, including subsidies, through guaranteed, long-term tariffs for electricity, contingent on their

---

[6] Canada enacted the Green Energy and Green Economy Act of 2008, which provided statutory support to the FiT program. *See* Green Energy and Green Economy Act, 2009, S.O. 2009, c. 12, Schedule B, *available at* http://www.ontla.on.ca/html/source/statutes/english/2004/elaws_src_s4023_e.htm

[7] REN21 Secretariat, *Renewables Global Status Report: Update* (2009).

[8] Panel Report, Canada - *Certain Measures Affecting the Renewable Energy Generation Sector*, WT/DS412/R, (Complainant - Japan) WT/DS426/R (Complainant – EU), (December 19, 2012). FiT program is applicable to projects generating more than 10kW, while the micro-FiT program targets individuals interested in small-scale projects not exceeding 10kW. The Ontario Power Authority (OPA) is responsible for managing and administering the FiT program in Ontario.

[9] M S Srikar, *Renewable Energy Programmes in the European Union, Japan and the United States: Compatibility with WTO Law*, Centre for WTO Studies (CWS) Working Paper # 200/4, (August 27, 2012), *available at* SSRN: http://ssrn.com/abstracts=2179621.

[10] The size of the individual grants ranged between $6.7 million and $22.5 million.

purchase and use of solar cells and solar modules of domestic origin.[11]

Renewable energy technologies such as solar, wind, geothermal and biomass power generation are gaining traction and popularity, but are not yet viable at a utility scale level to play a significant role in a country's energy mix. The inability to internalize the cost of greenhouses gas (GHG) emissions has caused significant underpricing of non-renewable forms of energy. This market failure has also resulted in significant sub-optimal production of renewable energy. Economic theory posits that public intervention may be required when market fails to provide desirable public goods or prevent negative externalities. A number of firms in the renewable energy sector face complex risks involving future changes in demand, pricing, grid connection to wider markets, cost return on capital and other key performance and regulatory risks. The renewable energy industry is still developing and the economic viability of most such projects is uncertain. In addition, the discovery of shale gas has the potential to slow the development of renewable sources of energy. A recent study by KPMG, a consulting firm, indicates that the energy industry's focus on developing shale gas and other unconventional sources of energy could disrupt the economic viability of renewable energy and could potentially take the focus away from this sector.[12] Notwithstanding the above scenario, a number of developed and emerging economies have committed themselves to the production of renewable energy (*See* Table I).

Table I: Top Five Producers of Renewable Energy

New Capacity	Hydropower Capacity	Solar PV Capacity	Wind Power Capacity	Biodiesel Production	Ethanol Production	Solar Hot water/heat
China	China	Italy	China	United States	United States	China
United States	Vietnam	Germany	United States	Germany	Brazil	Turkey
Germany	Brazil	China	India	Argentina	China	Germany
Italy	India	United States	Germany	Brazil	Canada	India

[11] Press Release, *United States Challenges India's Restrictions on U.S. Solar Exports*, (February 12, 2013), *available at* http://www.ustr.gov/about-us/pressoffice/pressreleases/2013/february/us-challenges-india-restrictions-solar.

[12] KPMG, *Shale Gas: Global Perspectives*, 19, (2011) *available at* http://www.gses.com/images/documents/shale-gas-global-perspective.pdf.

India	Canada	France	UK/ Canada	France	France	Italy

Source: REN21 Report (2012)

It is widely perceived that the market for renewable energy is unstable under present conditions and that some form of government support is generally desirable or justifiable. Strong government policies may be required to provide a predictable environment. However, a spate of antidumping and CVD measures on renewable energy parts and components and multiple challenges before the WTO against some of the renewable energy programs have raised the issue whether the current international trading regime is against renewable energy initiatives.[13]

This article examines the nature and characteristics of the renewable energy sector and explores the extent to which public or governmental support can be extended to the renewable energy sector. In particular, Section A examines how some of the governmental support to the renewable energy sector is constrained by the Agreement on Subsidies and Countervailing Measures (SCM Agreement).[14] Section B examines the compatibility of domestic content requirement in some of the renewable energy programs and examines how it comports with various WTO provisions including the Agreement on Trade-related Investment Measures (TRIMs Agreement).[15] Section C examines the applicability of General Exceptions under the GATT in justifying the violations of various covered agreements under the WTO. Section D concludes.

Renewable Energy and Subsidies

Subsidies to renewable energy sector operate at different levels and are given at different stages. In certain cases, governments may provide subsidies to producers of renewable energy whereas in other cases governments may subsidize consumers of renewable energy products. Certain countries provide rebate on electricity bills whereas others provide preferential tax credits, low interest loans or investment credits. In China, subsidies were provided to cover installation costs for both grid and off-grid connections, in addition to other benefits, such as cheap land,

[13] Joost Pauwelyn, *Global Challenges at the Intersection of Trade, Energy and the Environment* 5, (2010), *available at* http://www.cepr.org/press/CTEI-CEPR.pdf.

[14] Agreement on Subsidies and Countervailing Measures, (Adopted on April 15, 1994), Marrakesh Agreement Establishing the World Trade Organization, Annex IA, 1869 U.N.T.S. 14 [hereinafter SCM Agreement].

[15] Agreement on Trade-related Investment Measures, (Adopted on April 15, 1994), Marrakesh Agreement Establishing the World Trade Organization, Annex IC, 1868 U.N.T.S. 186 [hereinafter TRIMS Agreement].

preferential contracts from state-owned entities, and low interest government loans.[16] Governments may also use carbon taxes and other market based instruments.

Each of the above examples presents challenges that are unique. If subsidies are given to domestic renewable energy products as opposed to imported products it may clearly result in a violation of Article III, the national treatment provision of General Agreement on Trade and Tariffs (GATT).[17] On the other hand, tax credits or preferential loans at the behest of the government could involve a direct transfer of funds and can be easily classified as a subsidy, a practice regulated by the SCM Agreement.

Furthermore, renewable energy programs also differ widely in their scope and nature. FiT schemes have gained popularity in recent times and need a special discussion. Broadly, FiT schemes have a regulatory component and vary significantly in terms of their nature and design. FiT schemes generally ensure price certainty for the generators. The nature of the energy market in many countries is such that the government does not play an active role in the electricity market in producing, transmitting and distributing energy. However, under a FiT, a utility is contractually obliged to connect renewable energy generators to the grid and pay the generators for the electricity for the life of the FiT contract. In the case of most FiTs, the government does not make the payment directly, but only mandates a guaranteed tariff. The provision of a guaranteed price support is to encourage the RE sector. The FiT rates are not generally aligned with the market and the program costs may be very high; however, in such cases most of the FiT programs pass on the cost to the ratepayers.

It is an established fact that a large number of currently implemented FiT programs are disassociated from the market price. For example, eighteen out of the twenty-seven European Union member-states have adopted schemes guaranteeing minimum resale prices for renewably produced electricity. The fixed tariff is just the pricing element of the FiT incentive. In addition to this, FiT schemes include other terms either to reinforce the package of incentives, or to implement the program on a long-term basis.[18]

---

[16] Keith Bradsher, *To Conquer Wind Power, China writes the Rules*, N.Y.TIMES, (December 14, 2010). The steelworkers' petition cites various forms of subsidies and support that China has given to its industries in potential violation of international trade rules.

[17] Report of the Panel, *Italian Discrimination Against Imported Agricultural Machinery*, L/833, BISD 7S/60, (October 23, 1958).

[18] Luca Rubini, *The Subsidization of Renewable Energy in the WTO: Issues and Perspectives*, NCCR Trade Working Paper, (2011).

In examining the role of subsidies in encouraging clean and renewable energy programs, it is essential to examine the conflict between the role of the government and the distortionary impact of subsidies. In particular, all renewable energy programs will have to pass the test laid down by the SCM Agreement. The following discussion focuses on the concept of subsidy under the SCM Agreement and examines whether some of the renewable energy programs and, in particular, the FiT programs would raise concerns from the perspective of this Agreement.

Article 1.1 of the SCM Agreement provides a definition of the term "subsidy". According to Article 1.1, a determination of "subsidy" rests on satisfaction of two elements: (1) a financial contribution or income or price support by a public body; and (2) a conferral of "benefit" upon the recipient. The four types of "financial contribution" which are explicitly mentioned in Article 1.1 appear to be straightforward. They are:

- A direct transfer of funds;
- Government revenue that is "otherwise due" is foregone or not collected.
- A provision of goods or services or the purchase of goods or services by a government; and
- A government payment to a funding mechanism, or where the government entrusts or directs a private body to carry out a particular policy.

In addition to the above two requirements, a subsidy has to be meet the "specificity" test to fall under the disciplines of the SCM Agreement. A subsidy can qualify as "specific" in two different ways. Under Article 3 of the SCM Agreement, all export subsidies are import substitution subsidies are specific. Other subsidies can also be specific if they meet with the criteria under Articles 2.1 and 2.2 of the SCM Agreement.[19]

The financial contribution should from the government or a public body. One of the critical issues involved in the debate is the definition of a 'public body'. A WTO panel in *Korea-Commercial Vessels* pronounced that an entity is a public body when the government controls it.[20] More recently, the Appellate Body in *United States-AD/CVD*[21] decided that the evidence of a controlling interest itself

[19] Where a subsidy is explicitly limited to a sector or a region, either by the granting agency, or by legislation, it is *de jure* specific. On the other hand, where the authority or legislation establishes objective criteria or conditions governing the eligibility for, and amount of a subsidy, specificity shall not exist, provided that the eligibility is automatic and the criteria and conditions are strictly adhered to. *See* SCM Agreement, art 2.

[20] Panel Report, *Korea – Measures Affecting Trade in Commercial Vessels, WT/DS273/*R, (April 11, 2005).

[21] Appellate Body Report, *United States- Definitive Antidumping and Countervailing Duties on Certain Products from China*, ¶ 290, WT/ DS 379/AB/R (March 25, 2011).

is not sufficient to establish that an entity is a public body. According to the Appellate Body, "meaningful [governmental] control over an entity and its conduct may serve … as evidence that the relevant entity possesses governmental authority and exercises such authority in the performance of governmental functions." What is of relevance is whether the function of providing guaranteed tariff for renewable energy or enforcing a different type of renewable energy program is "normally vested" in the government, i.e., whethe the government would have normally performed this function instead of directing private entities to undertake it.

Assuming that government's role in renewable energy programs is quite prominent and uncontestable, it may be possible to establish that most of the government utilities or other funding agencies established and controlled by the state would qualify the definition of a public body.

It is also important to consider that financial contribution can be either direct or indirect. Mostly, in the case of FiT programs, a financial contribution presumably arises when the concerned governmental agency signs the FiT contract with the FiT generator and agrees to provide guaranteed rates. A direct transfer may arise when the public body transfers the difference between the market rate of electricity that the generator would receive under the standard operation of the market and the rate guaranteed under the FiT contract. Under the FiT contract, the FiT generators commit to supply the generated electricity into the grid in exchange of payment of the agreed rates. Such generation of electricity is expected in order to obtain the guaranteed rate, which provides in itself a benefit to the FiT generator. The panel noted in *EC-Large Aircraft* as follows:

> [W]hen assessing whether a transaction involves a "potential direct transfer of funds", the focus should be on the existence of a governmental practice that involves an obligation to make a direct transfer of funds which, in and of itself, is claimed and capable of conferring a benefit on the recipient that is separate and independent from the benefit that might be conferred from any direct transfer of funds. This can be contrasted with financial contributions in the form of direct transfer of funds, which will result in a benefit being conferred on a recipient when there is governmental practice that involves a direct transfer of funds.[22]

Another interesting issue is whether the FiT schemes involve a purchase of electricity by any public body within the meaning of Article 1.1 (a) (i) (iii) of the SCM Agreement? A clear answer to this question would depend on the type of the underlying FiT arrangement or model. Nonetheless, it appears that if the concerned public body dealing with the energy sector pays or undertakes to pay

---

[22] Panel Report, *European Communities and Certain Member States- Measures Affecting Large Civil Aircraft*, ¶ 7.304, WT/DS 316/R (1 June, 2011) (as modified by the Appellate Body).

a certain price (which includes the FiT) as a consideration for the delivery of electricity into its transmission network which it owns and controls, it involves a sale and purchase transaction. Assuming that electricity is a good,[23] the essence of a bilateral contractual transaction between the public body and the renewable energy generators could properly place this transaction as a "purchase of goods" within the meaning of Article 1.1 (a) (i) (iii) of the SCM Agreement. To that extent, the characterization of this transaction as a "purchase of goods" appears more appropriate than an unqualified "transfer of funds". The WTO panel in *Canada-Renewable Energy* observed that a FiT or micro FiT program, as implemented in that case, could be appropriately characterized as a "government purchase of goods".[24]

Article 1.1(a)(1)(iv) also encompasses the case in which a government "entrusts or directs" a private body to effectuate a financial contribution as understood to carry out one or more of the functions enlisted in para (i)—(iii) of Article 1.1 (a) (i) of the SCM Agreement (hence encompassing the scenario where a private energy provider is entrusted to run a FiT program by government). For example, in Germany, the Erneuerbare-Energien-Gesetz(EEG) statutorily "directs" the private parties to purchase electricity sourced by renewable energy technologies.[25] This type of a scenario may not involve a cost to the government, but nonetheless could satisfy the requirements of a financial contribution.

Even if a government's involvement in the RE sector does not amount to a financial contribution, it can be found as an "income or price support" within the meaning of Article 1.1 of the SCM Agreement or Article XVI of the GATT. The term "support" is often used in the context of agriculture, especially with respect to government support programs for farm products. In the ordinary meaning, "support" denotes "the action of contributing to the success or maintaining the value of something". In the light of this ordinary meaning, the meaning of "support" within Article 1.1 (a) (2) refers to the action of the government that directly or indirectly increases the export of any product from its territory or reduces the imports of any product within its territory. The Appellate Body in *United States- Softwood Lumber* noted that the range of government measures capable of providing subsidies is broadened still further by the concept of "income or price

[23] There is no affirmative finding on this issue, but the WTO panel seems to have acknowledged this fact.

[24] Panel Report, *Canada- Renewable Energy Generation Sector*, *Supra* note 8 at ¶ 7.11.

[25] Germany's FiT program is one of the few FiT programs that do not rely upon a public body or State actor for the provision and management of FiT payments. *See* Laird and Stefes, *The Diverging Paths of German and United States Policies for Renewable Energy: Source of Difference*, 37 ENERGY POLICY 2619, 2624 (2009).

support" in paragraph (2) of Article 1.1(a).[26] Some academic commenters also suggest that the expression "income or price support" falling under Article 1.1 (a) (2) of the SCM Agreement could be a better alternative to the expression "financial contribution" appearing in Article 1.1 (a) (1) in properly characterizing and dealing with most FiT schemes.[27]

In the light of the discussion above, it appears almost certain that most government intervention either under a FiT scheme or direct support will fall under one of the gateways provided under Article 1.1 of the SCM Agreement. In other words, most government intervention could be characterized either as a "financial contribution" or as a form of "income or price support" under Article 1.1 of the SCM Agreement.

The second essential element required for the determination of a subsidy is the conferral of "benefit". The term "benefit" in Article 1.1(b) implies a financial contribution that places the recipient in a more advantageous position than would have been the case but for the financial contribution. It means that a financial contribution will only confer a "benefit", i.e., an advantage, if it is provided on terms that are more advantageous than those that would have been available to the recipient in the market.[28] As the *Canada- Aircraft* panel reiterated, the existence of "benefit" (in the context of financing) is determined by reference to the terms at which similar financing is available to the customer in the market.[29] In *EC-DRAMS*, the WTO Panel noted that the existence of a benefit is a constitutive element of the definition of a subsidy. The panel also noted, "…only in cases where the financial contribution provides the recipient with an advantage over and above what it could have obtained on the market will the government's financial contribution be considered to have conferred a benefit and will a subsidy thus be deemed to exist."[30] The panel further clarified, "if the public or publicly directed financial contribution is provided under the same conditions as a private market player would have provided, then there would be no reason

---

[26] Appellate Body, *United States- Final Countervailing Duty Determination with Respect to Certain Softwood Lumber from Canada*, ¶52, WT/DS 257/AB/R (Feb. 17, 2004).

[27] LUCA RUBINI, THE DEFINITION OF SUBSIDY AND STATE AID, WTO AND EC LAW IN COMPARATIVE PERSPECTIVE (2009). There is a contrary view that price regulation in the context of utilities or network industries ought not to be considered as a price support under Article 1.1 (a) (2). *See* Robert Howse, *Climate Mitigation Subsidies and the WTO Legal Framework: A Policy Analysis* 12-13 (International Institute of Sustainable Development, Trade, Investment and Climate Change Series) (2010).

[28] Appellate Body Report, *Canada – Measures Affecting the Export of Civilian Aircraft*, ¶ 154, WT/DS70/AB/W (Adopted on August 20, 1999) [hereinafter *Canada- Aircraft*].

[29] Panel Report, *Canada – Measures Affecting the Export of Civilian Aircraft – Recourse by Brazil to Article 21.5 of The DSU*, ¶ 9.112, WT/DS70/RW, WT/DS70/AB/RW (Adopted on August 4, 2000).

[30] Panel Report, *European Communities – Countervailing Measures on Dynamic Random Access Memory Chips from Korea*, ¶7.175,WT/DS299/R (Adopted on August 3, 2005)[hereinafter *EC- DRAMS*].

to impose any discipline, simply because the financial contribution was provided by the government."

The relevant benchmark for the purpose of determining the existence of a benefit is the market. The Appellate Body in *EC- Large Aircraft* noted as follows:

The market place to which the Appellate Body referred to in *Canada- Aircraft* reflects the sphere in which goods and services are exchanged between willing buyers and sellers. A calculation of benefit in relation to prevailing market conditions thus demands an examination of behavior on both sides of a transaction, and in particular, in relation to the conditions of supply and demand as they apply to that market.[31]

The generators of renewable energy might seek a return on their investment to cover their costs. In most of the FiT programs, the prices in the price schedule are intended to cover development costs plus a reasonable rate of return projects. Furthermore, the fact that the public body imposes fees and charges on consumers to recoup the high costs involved in the generation of the electricity through the FiT program indicate that that the electricity generated through the FiT program would not be sold without the FiT program.

In the *Canada- Renewable Energy* dispute, Japan and the European Union argued that the FiT price exceeded various wholesale electricity market price benchmarks (inside and outside Ontario). They also argued that the very nature and objectives of the FiT program are intended to facilitate private investment in renewable electricity generation that the market would not otherwise provide. Canada, however, defended its measure arguing that the benefit analysis should be made with reference to the 'market' for electricity produced from wind and solar PV technologies, and not to benchmarks - such as those suggested by Japan and the EU - which reflect a single price for electricity, irrespective of its origin.

In regard to the determination of "benefit" the majority Panel agreed with Canada to the effect that Ontario's wholesale electricity market cannot offer any reliable benchmark because it is distorted by the government. The majority Panel concluded that there is no benefit, and consequently no subsidy, because there would not have been any similar investment in the market, i.e. an investment delivering the same goods as desired by Ontario (what the Panel describes as

[31] Appellate Body, *European Communities and Certain Member States- Measures Affecting Trade in Large Civil Aircraft*, ¶ 981, WT/DS 316/AB/R (June 1, 2011)[hereinafter *EC- Large Civil Aircraft*].

the 'missing money problem').[32] The panel noted that if the price achieved on the "organized" wholesale market is not allowed to rise to a level, which fully compensates generators for the all-in cost their investment (both fixed and sunk costs), private investors will not be willing to finance construction of new electricity generation under such conditions.[33] In the panel's view, alternative mechanisms to wholesale spot markets was required to provide long term investment to meet forecasted demand.[34]

Some of the rationale provided by the panel to determine the consistency of the subsidy aspects of the FiT program may be reviewed or modified by the Appellate Body. It seems almost self-evident that without the FiT program market forces in Ontario (and possibly in other parts of the world as well) would not lead to the reliable supply of renewable energy electricity which is desired for environmental and energy goals.[35]

In conclusion, in the renewable energy sector, the delineation of the market and the choice of the appropriate benchmarks for benefit determination will remain contentious. This debate will essentially determine the extent to which governments could subsidize renewable energy programs. It needs to be, however, reiterated that not all renewable energy subsidies are *per se* prohibited. However, if a subsidy is contingent upon the use of domestic over imported goods, such a requirement could convert the subsidy into a prohibited subsidy. The Canada FiT program is one such category where the FiT generator was required to purchase or use energy generation equipments and components that are of Canadian origin or from a Canadian source. In other words, if renewable energy subsidies do not fall within category, i.e. under Article 3 of the SCM Agreement, the existence of adverse effects[36] is essential for applying the other disciplines of the SCM Agreement to these categories of subsidies. Furthermore, a subsidy must be specific to certain industries or enterprises in order to be actionable under the SCM Agreement.[37] A number

---

[32] Panel Report, *Canada- Renewable Energy*, *supra* note 8, ¶ 7.283.

[33] *Id.*

[34] *Supra* note 32

[35] *Supra* note 32 at ¶ 7.284 (the Panel notes that because of the specific features of electricity and the nature of competitive wholesale electricity markets, government intervention will often be necessary in order to secure an electricity supply that is safe, reliable and sustainable in the long-term).

[36] The various tests for adverse effects can be found in Article 5 and 6 of the SCM Agreement: (i) injury to the domestic industry, (ii) nullification and impairment of benefits, i.e. tariff concessions, and (iii) serious prejudice in various forms mainly of displacement and price effects in various markets.

[37] *See Supra* note 14. In terms of Article 2.1(b) of the SCM Agreement, a subsidy cannot be specific if the eligibility for the subsidy depends on 'objective criteria or conditions', i.e criteria or conditions which are neutral, which do not favour certain enterprises over others, and which are economic in nature and horizontal in application, such as number of employees or sizes of enterprises'.

of antidumping and countervailing duty actions have come up against various forms of state support given to parts and equipments used for renewable energy production.[38] But these trade contingent actions are unlikely to stop government intervention in the renewable energy sector. So long as the renewable energy subsidies do not fall within the prohibited category, the WTO members will have some leeway in implementing government subsidies, albeit in a selective way.

Section B examines the nature and WTO consistency of domestic content requirements in some of the renewable energy programs.

Renewable Energy and Trade-related Investment Measures

The SCM Agreement prohibits export subsidies and other types of subsidies that are conditioned on the use of domestically manufactured products. Subsidies that impose purchase obligations based on the origin of energy or technology can be a prohibited subsidy and can fall foul of the obligations under the TRIMs Agreement.

According to development scholars, export subsidies and local content requirements were key elements in the industrialization of number of "late industrializers".[39] Similar arguments are raised in relation to local content requirements in renewable energy programs. Local content requirements are widely considered as effective tools in industrial policy in as much as they ensure steady and fast development of an important and newly emerging domestic renewable energy sector.[40] A number of renewable energy programs require use of local content to encourage the local firms to either promote the domestic manufacturing sector or to create employment.[41]

---

[38] *U.S. Sets Antidumping Duties on Chinese Solar panels*, BLOOMBERG NEWS, (October 11, 2012); In the case of China, the NME methodology under the antidumping measure is used as a proxy to deal with various types of subsidization as well. *See also* http://about.bloomberglaw.com/practitioner-contributions/wave-of-trade-disputes-complicates-global-market-for-renewable-energy-firms-particularly-solar-sector.

[39] Alvaro Santos, *Carving Out Policy Autonomy for Developing Countries in the World Trade Organization: The Experience of Brazil and Mexico*, 52 VA. J. INTL. L. 551, 561 (2012) (arguing that TRIMS Agreement is not too stringent in practice in enabling developing countries to maintain their local content requirements in important sectors).

[40] Dani Rodrik, One Economics, Many Recipes: Globalization, Institutions and Economic Growth (2008).

[41] Since 2005, Brazil has required that at least 60 percent of the total cost of wind energy products is sourced from Brazil. A number of EU countries have also implemented local content requirements in the renewable energy sector. In 2011, Italy has enacted local content requirements in their legislation for subsidization of solar energy based on the sourcing of renewable energy equipments and components. In 2012, France imposed a local content requirement wherein the government offers a 10% bonus on the price that Electricite de France (EDF) pays to the solar energy installers. The bonus is available only when 60% of the added value of the installed solar panels is generated within the EU. Again, in the United States, several states including Montana and Louisiana have a local content rule in their blending mandate for bio-fuels. *See* Jan- Christph Kuntze & Tom Moerenhout, *Local Contents Requirements and the Renewable Energy Industry: A Good Match*? (September 12, 2012), *available at* SSRN: http://ssrn.com/abstract=2188607.

Especially in the cases of countries such as China, the local content rules are considered to have been successful in helping transfer of technology and knowhow. It is reported that in the field of wind turbine equipment manufacturing industry, the five largest Chinese companies had growth rates of more than 113%.[42]

In most renewable energy programs involving local content requirements, the government provides subsidies in the form of tax rebates or credits contingent upon compliance of local content requirements. In particular, some of the state sponsored renewable energy support programs require that the concerned energy equipments are manufactured or principally manufactured in certain parts of the state or specific percentage of manufacturing or assembling is carried out in that region or by using domestic feedstock, etc.[43]

Local content requirements in the context of FiT programs are particularly problematic. FiT schemes are different from other renewable energy programs in as much as they may have heavy project costs and longer gestation periods. For most such programs to be politically feasible, it may be important to encourage local employment creation. Therefore, even if it is admitted that local content requirements have inefficient outcomes in the long run, it will be politically difficult for most governments to set apart government funds for green energy programs. Beyond this, most local content requirements, at least, indirectly support green industries- an objective that is laudable in itself. For example, the Canadian Minister's FiT Directive to the Ontario Power Board lists various objectives that, *inter alia*, include measures to "[e]nable green industries through new investment in renewable energy technologies".[44]Therefore, global technological innovation in renewable energy could be considered as a public good, which could significantly outweigh the baneful effects of local content or import substitution policies.

In the above context, a key consideration is whether the existing WTO framework provides flexibilities for local content policies in renewable energy programs. The only point of enquiry is whether the FiT program discriminates against the imported renewable energy generation equipment products vis-à-vis domestic products. If it does discriminate, such a measure may fall within the blanket prohibition under the TRIMs Agreement as could be evident from the following

---

[42] *Id.*

[43] *See* World Trade Organization, Certain Local Contents in Some of the Renewable Energy Programs, Questions by India to the United States, G/TRIMS/W/117 (April 17, 2013).

[44] George Smitherman, *Ontario Legislative Assembly Debates* (Hansard), 39th Parliament First Session, (February 23, 2009), 4937, 4952, *available at* http://www.ontla.on.ca/web/house-proceedings/house_detail.do?Date=2009-0223&Parl=39&Sess=1&locale=en#P388_90530 (highlighting Ontario's policy on renewable energy and energy conservation).

treaty provisions.

Article 2.1 of the TRIMs Agreement provides that:

Without prejudice to other rights and obligations under GATT 1994, no Member shall apply any TRIM that is inconsistent with the provisions of Article III or Article XI of GATT 1994

Paragraph 2 of Article 2 in turn states that:

An illustrative list of TRIMs that are inconsistent with obligation of national treatment provided for in paragraph 4 of Article III of GATT 1994 and the obligation of general elimination of quantitative restrictions provided for in paragraph 1 of Article XI of GATT 1994 is contained in the Annex to this Agreement.

Paragraph 1(a) of the Annex to the TRIMs Agreement states that:

TRIMs that are inconsistent with the obligation of national treatment provided for in paragraph 4 of Article III of GATT 1994 includes those which are mandatory or enforceable under domestic law or under administrative rulings, or compliance with which is necessary to obtain an advantage, and which require:

(a) the purchase or use by an enterprise of products of domestic origin or from any domestic source, whether specified in terms of particular products, in terms of volume or value of products, or in terms of a proportion of volume or value of its local production.

A number of renewable energy programs including FiT schemes make it obligatory on the generators to purchase or use a sufficient proportion of domestic goods or to meet the minimum required domestic content in order to receive the guaranteed, long-term rates under the FiT scheme. If there is a preference for domestic goods over imported goods for availing a benefit, it is more than sufficient to hold that that such a requirement is a prohibited TRIM.

Considering the zero tolerance that the GATT treaty and the TRIMs Agreement have shown to domestic content requirements, a number of well-meaning subsidies are *per se* considered as prohibited. However, there is a disconnect here, between the WTO legal standard and the renewable energy policies of a vast majority of WTO members. Domestic content requirement are highly pervasive and various federal, sub-federal and municipal units establish domestic content

requirements or "buy local" provisions to receive government support.[45] It will be inconceivable at this stage to negotiate flexible standards in regard to domestic content use either in the TRIMs Agreement or any other multilateral framework. It is necessary to find the flexibility somewhere else. Section C examines the availability of policy space under the WTO.

Renewable Energy and Lack of Policy Space under the WTO

Both the SCM Agreement and the TRIMs Agreement work in a fairly rigid and inflexible way at present, in the absence of clearly spelt out exceptions for environmental purposes. The "green-light" subsidies, i.e., the government measures that deemed certain governmental assistance non-actionable under the SCM Agreement expired at the end of 1999 given the lack of consensus among the WTO Members to extend them.[46] The Agreement on Agriculture (AoA) had a "due restraint" clause (commonly referred to as the "Peace Clause") in Article 13, which exempted green box measures from countervailing actions and multilateral challenge under the SCM Agreement during the implementation period. Although there is a clamour for reinstating such a safe haven for the purpose of promoting renewable energy or for climate change mitigation or adaptation, for all practical purposes, no formal decision has been taken for extending such flexibility. Therefore, no subsidy is immune from challenge for the time being.

In the absence of specific exceptions, WTO Members can only turn to general exceptions under the GATT. Article XX of the GATT 1994 provides exceptions for measures "necessary to protect human, animal or plant life or health" or "relating to the conservation of exhaustible natural resources". Article XX (b) permits the adoption of measures that are "necessary to protect human, animal or plant life or health" and has been used in several WTO disputes. This exception is not limited to public health policy measures, but also covers 'environmental' measures. In *Brazil-Tyres*, the Appellate Body commented that Article XX(b) could also include climate change measures.[47] Article XX (g) of the GATT, on the other hand, permits the adoption of measures that are related to the conservation of exhaustible natural resources, provided that such measures are made

---

[45] *Supra* note 9 (listing the RE programs of specific countries and a detailed account of various TRIMs requirements).

[46] SCM Agreement, art 3. The SCM Agreement as it originally entered into force contained a third category — non-actionable subsidies. This category (along with a provision establishing a presumption of serious prejudice in respect of certain specified types of actionable subsidies) applied provisionally for five years ending 31 December 1999, and pursuant to Art. 31 of the Agreement could be extended by consensus of the SCM Committee. As of 31 December 1999, no such consensus had been reached.

[47] Appellate Body Report, *Brazil-Measures Affecting Imports of Retreaded Tyres*, ¶224, WT/DS332/AB/R (December 3, 2007); *see also* Christopher Tran, Using GATT, Article XX to justify Climate Change Measures in Claims under the WTO Agreements, 27 ENV'L & PLANNING LAW J., 346 (arguing how climate change measures can pass muster under Article XX).

effective in conjunction with restrictions on domestic production or consumption. In WTO dispute settlement, this provision was first invoked in *US- Gasoline,* where it was determined that "a policy to reduce the depletion of an exhaustible natural resource" was within the meaning of Article XX (g).[48]

In the context of renewable energy one of the key questions is whether a WTO member can successfully avail the general exceptions under Article XX of the GATT. In other words, can Article XX justify a violation to Article 3.1(b) of the SCM Agreement given the absence of a specific provision? This is an unresolved and lively issue and there are differing opinions on the applicability of Article XX.

The WTO Appellate Body in *China- Audiovisual*[49] ruled that the applicability of Article XX beyond the GATT framework could not be excluded altogether. This particular reasoning was rejected by the Appellate Body in *China- Raw Materials.*[50] In any case, this will be an issue that has to be examined case-by-case, agreement-by-agreement, or accession protocol-by-accession protocol. The question whether GATT Article XX could apply in respect of other Annex IA Agreement was also addressed in the recent dispute of *United States- Poultry.*[51] The WTO panel was of the view that a measure that was already found to be in violation of the SPS Agreement, and which expressly incorporates Article XX (b) of the GATT, could not be justified by having direct recourse to Article XX (b) of the GATT. Therefore, a more conservative view would limit Article XX exceptions generally to GATT 1994 and not to other Annex IA Agreements, which broadly come under the category of *lex specialis.*

The availability of general exceptions and exemptions is key to enabling the WTO members to preserve their policy space in areas such as renewable energy. The lack of a negotiating mandate for a substantive agreement on renewable energy subsidies within the WTO accentuates this difficulty for WTO members to encourage renewable energy programs. However, it looks improbable, in the absence of clear textual support, that the Appellate Body would accept a defence

---

[48] Appellate Body Report, *United States- Standards for Reformulated and Conventional Gasoline*, ¶ 14, WT/DS2/AB/R, 20, (April 29, 1996) [hereinafter US- Gasoline].

[49] Appellate Body Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶83, WT/DS363/AB/R, (December 21, 2009).

[50] Appellate Body Report, *China- Measures Related to the Exportation of Various Raw Materials*, WT/DS 394/AB/R, WT/DS395/AB/R, WT/DS 398/AB/R, ¶303 (January 30, 2012) [hereinafter *China- Raw Materials*].

[51] Panel Report, *United States- Certain Measures Affecting Poultry from China*, WT/DS 392/R, ¶ 4.116. (September 29, 2010),

under Article XX for a violation of a prohibited subsidy under the SCM Agreement or an illustrative TRIM under the TRIMs Agreement. As one commentator put it, it will be unreasonable to expect a panel or Appellate Body to adopt a "heroic approach to interpretation" to fill this void.[52]

Conclusion

The renewable energy sector has a crucial role in ensuring energy security and in addressing concerns of climate change. The dependence on fossil fuel based energy resources will have to be progressively reduced. It is, therefore, essential that rules of international trading system, which were crafted almost two decades ago, are interpreted in an evolutionary manner.

There is at least some evidence that well targeted subsidies themselves are not a significant area of concern in the field of renewable energy, but it is the provision of subsidies tied to the use of domestic inputs and renewable energy equipment over imported goods that make some of the renewable energy programs prohibited subsidies. Whatever be the economic merits in prohibiting such practices, it is important to secure political support for renewable energy programs and to attract investors to make long-term investments in this field. Domestic content requirements and local employment creation could be reasonable means for encouraging investment in this field. This paper has, however, argued that the room for flexibility in trade rules at present is very limited. The lack of specific exceptions and exemptions under the SCM Agreement and the TRIMs Agreement will create insuperable difficulty for the implementation of various renewable energy programs.

Given this lack of flexibility under the GATT, SCM and TRIMS Agreements, judicial organs of the WTO are likely to spend considerable time in interpreting the meaning of rather plain treaty texts or common terms such as "financial contribution", "benefit", "advantage" and their different variants under the SCM Agreement or such similar expressions under the GATT or the TRIMs Agreement in the future. It would have been far more desirable had a sectoral or stand-alone agreement on renewable energy was agreed upon to avoid these complexities. However, until a long-term framework is identified and agreed upon, the WTO panels and Appellate Body will have to carefully tread the field of renewable energy and international trade regulation. A false step taken in this direction could completely unsettle several renewable energy programs and could foil fresh

[52] Condon, *Climate Change and Unresolved Issues in WTO Law*, 12 J. INT'L ECON. L. 895, 911-913 (2009).

initiatives taken in this field.

SHOULD THE LAW BEAT A RETWEET? RATIONALISING LIABILITY STANDARDS FOR SHARING OF DIGITAL CONTENT

Nandan Kamath[*]

The emergence of social media has raised new and interesting questions concerning the regulation of free speech. One such question is the legal treatment of the sharing of third party digital content. Using the example of a 'retweet', this article highlights the urgent need to establish clearer liability standards for those sharing, repeating or endorsing illegal or infringing content. It attempts to propose a clear, principle-based approach that lifts the cloud of uncertainty creating a chilling effect on speech.

This act of retweeting is sought to be analysed against various legal frameworks including defamation, copyright infringement and public order. It is seen that unlike an intermediary that enjoys safe harbour protection, the retweeeter is treated on par with a principal actor. The law as it stands today does not differentiate between the repetition and original posting of content. This has a chilling effect on the act of sharing and reduces the diversity of voices on the internet. For these reasons, it is argued that a retweeter must be protected as a traditional internet intermediary. Finally, this article postulates a legal framework for attributing liability to the retweeting of illegal and infringing content that accounts for the unique context of social media communications.

Introduction

> "*Technologies that greatly empower people to communicate are transformative enough to cause injury… The internet can help us understand and own the ethical dimensions of what we do online, and to make morally informed, rather than legally compelled, choices about the information we absorb and refract onward.*"
>
> – Jonathan Zittrain[1]

Laws the world over have approached the regulation of new technologies with varying degrees of sophistication. The treatment of content distributed via social media platforms is a prime example. The laws of India have yet to achieve a nuanced balance between protecting freedom of speech on social media and regulating speech that is illegal or infringing.

Recent incidents of users being arrested and charge sheeted for alleged offences under the Information Technology Act, 2000 and related laws for the act of merely "liking" a third party's

---

[*] Nandan Kamath is a graduate of the National Law School of India University, the University of Oxford (on a Rhodes Scholarship) and Harvard Law School. He is Principal Lawyer at LawNK - The Law Offices of Nandan Kamath, a boutique sports, entertainment and intellectual property law practice based in Bangalore. His clients include a number of international and national sports bodies, athletes, sponsors and artists as well as brand and content driven businesses.

[1] Jonathan Zittrain, *A Twitter law would be unwise*, THE FINANCIAL TIMES, November 23, 2012, *available at* http://www.ft.com/cms/s/0/f7aff27a-33f1-11e2-9ce7-00144feabdc0.html.

post[2] have highlighted the urgent need to establish clearer liability standards for those sharing or endorsing illegal or infringing content. That most of the cases pursued by those enforcing the law have had politicians and their kin as the subject matter of the impugned speech only reinforces the need for carefully protecting free speech in the online context.

Social media tools enable online conversations and facilitate the effective relaying of information that enriches our social and political domain. The same mechanisms also provide a platform for the dissemination of defamatory content, lies and incendiary content that can cause personal and public harm of significant proportions. A balance must be found that effectively attaches culpability to clearly illegal and infringing acts without concurrently hindering the legitimate use of these services.

This article uses the example of the retweet, evaluating the current and potential legal treatment of this message sharing feature of the Twitter service. This is used to exemplify how we would be well advised to not stigmatise the increasingly novel means of sharing of third party digital content and dis-incentivise the users facilitating such dissemination. While the laws of India are the primary subject matter of the article, the conclusions arrived at could apply equally to practically every legal system worldwide. This article makes a call for a clear, principle-based approach that lifts the cloud of uncertainty chilling speech rather than protecting it.

What is Twitter?

Twitter is an online social networking and micro-blogging service.[3] It permits its users to post and read text-based messages (called "tweets") of up to 140 characters each.[4] With over 500 million registered users and 200 million active users as of 2012,[5] it relays approximately half a billion user-generated tweets on a daily basis.[6] These tweets are on practically every subject under the sun.

Tweets can be posted and read via text messages, web browsers, compatible desktop applications and mobile application services, which enable "always on" and "on the move" Twitter access. With

---

2 *A Facebook 'like' could land you in jail - courtesy Section 66A of IT Act*, November 20, 2012, *available at* http://www.sify.com/news/a-facebook-like-could-land-you-in-jail-courtesy-section-66a-of-it-act-news-national-mluoPDhcedh.html

3 *See* www.twitter.com.

4 *See* https://support.twitter.com/articles/215585-twitter-101-how-should-i-get-started-using-twitter#.

5 Lisa O'Carroll, *Twitter active users pass 200 million*, December 18, 2012, THE GUARDIAN, *available at* http://www.guardian.co.uk/technology/2012/dec/18/twitter-users-pass-200-million.

6 Daniel Terdiman, *Report: Twitter hits half a billion tweets per day*, October 26, 2012, CNET, *available at* http://news.cnet.com/8301-1023_3-57541566-93/report-twitter-hits-half-a-billion-tweets-a-day/.

a click of a button, registered users can post tweets. Each tweet is, by default, immediately publicly viewable, searchable and readable by anyone with access to the Twitter website, via third party applications and on other websites embedding these tweets.

What is a retweet?

In short, a retweet is a re-posting or sharing by a registered Twitter user of someone else's tweet.[7] The retweet appears on the re-poster's Twitter profile timeline. It is possible for a user to retweet posts made not only by those users he or she "follows" but also those made by any other Twitter user posting on the service, in each case except where the original poster has a "protected account".[8]

Retweets include the name and profile photo of the original poster and are accompanied by a retweet icon and text information stating that the post is a retweet by the retweeting poster.[9] Though not an official Twitter command or feature, Twitter users have also conventionally manually typed RT and the original poster's Twitter handle at the beginning of a tweet to indicate that they are re-posting and quoting someone else's tweet[10] (e.g., 'RT @originalposter This is the original tweet').

Where a tweet is reproduced verbatim with the RT prefix or has been retweeted without modification or addition, such a retweet is commonly known as a 'naked' retweet. This is to be distinguished from the 'modified' retweet (often used with the prefix MT), which re-posts a modified, edited or truncated version of the original poster's tweet, potentially altering its meaning and context.

The subject matter of this article is the accurate and complete 'naked' retweet reproduced without modification. The principles herein would apply equally to a retweet prefixed with additional comments from the retweeter that are not themselves independently infringing (e.g., 'I agree with this. RT @originalposter: This is the original tweet'). Though it has its own unique characteristics, culture and social context, a retweet is in all material aspects, functionally equivalent to sharing, re-

---

7 *See* https://support.twitter.com/groups/31-twitter-basics/topics/109-tweets-messages/articles/20169873-how-to-retweet-a-tweet#.

8 *See* https://support.twitter.com/articles/77606-faqs-about-retweets-rt#.

9 *See* https://support.twitter.com/groups/31-twitter-basics/topics/109-tweets-messages/articles/20169873-how-to-retweet-a-tweet#.

10 *Id.*

posting or liking a third party's Facebook post or the act of sharing on a number of other similar social media platforms.

Why do retweets matter?

The effect of a retweet is that the content of the original tweet is repeated as is and, consequently, is amplified to a larger number of viewers than only the followers of the original poster.

The retweet is variously seen as social currency, endorsement and a badge of the quality and resonance of the particular original posting. It is also used as a mode of content dissemination,[11] to amplify a statement or a point of view, to curate and filter third party content, to build friendships and reinforce relationships, to gain followers and prominence and also to reciprocate an act of retweeting by another user.[12] Retweeting, like most other digital sharing activity, can occur with a single click, a trivial, momentary action. The underlying content most often has a casual and conversational tenor.[13]

Despite all of its informality, Twitter has emerged as a content publication platform of note. Although almost exclusively carrying user generated third party content, it is increasingly relied on as a genuine and current source of news as well as crowdsourced opinion and interactive social commentary.[14] At the same time, its tenor is spontaneous and conversational[15] with a significant proportion of the content being characterised as "pointless babble".[16]

Attributing legal liability

By virtue of laws protecting traditional internet intermediaries,[17] there is no single entity, such as Twitter, that can be held responsible for all the content that is published on this publicly viewable and searchable platform. The safe harbours enjoyed by internet intermediaries are premised on

---

[11] Sarosh Khan, *The Threat Posed to Reputation by the Emergence off Social Web Technologies,* 23 ENT. L.R. 5, 126 (2012).

[12] *See* Daxton R. Stewart, *When Retweets Attack: Are Twitter users liable for republishing the defamatory tweets of others?,* 32 (2012), *available at* http://works.bepress.com/daxton_stewart/7.

[13] *Supra* note 1.

[14] Ellyn M. Angelotti, *Twibel Law: What Defamation and Its Remedies Look Like in the Age of Twitter*, 24, (2012), *available at* http://works.bepress.com/ellyn_angelotti/1.

[15] Jacob Rowbottom, *To Rant, Vent and Converse: Protecting Low Level Digital Speech,* 71 C.L.J. 2, 355 (2012).

[16] According to a study conducted by Pear Analytics, 40% of all tweets are pointless babble. *See* http://www.pearanalytics.com/blog/2009/twitter-study-reveals-interesting-results-40-percent-pointless-babble.

[17] *See*, for example, §79 of the Information Technology Act, 2009 and the Information Technology (Intermediaries guidelines) Rules, 2011 in India and §512 of the Digital Millennium Copyright Act, 2000 and §230 or the Communications Decency Act in the US.

them being passive conduits and carrying and hosting user generated content that they do not control. There is no equivalent legal immunity for those sharing the content. Twitter, in fact, puts users on notice that they not only own but are responsible for the content they post.[18] While the legal standards for attributing liability to original tweeters for infringing content are progressively evolving, those relating to sharing and re-posting of this content are less clear.

A couple of hypothetical cases are useful to frame the issues:

Case A: An Opposition Member of Parliament tweets to his 200,000 followers "*This Prime Minister is the most corrupt leader our country has ever had. A Swiss bank account, 5 undisclosed offshore properties*". His tweet is read by tens of thousands of Twitter users, with over 5,000 of them retweeting "*RT @OppnMP This Prime Minister is the most corrupt leader our country has ever had. A Swiss bank account, 5 undisclosed offshore properties.*" The Opposition MP is sued for defamation by the Prime Minister and is unable to prove the truth of his statements. Should the 5,000 retweeters also be held liable for publishing defamatory content about the Prime Minister?

Case B: To the official Twitter account of the anchor of a leading TV news channel is posted "*Communal clashes in the capital, 25 killed*". The 500,000 followers of this account view this tweet. Over 25,000 of them retweet "*RT @TV Anchor Communal clashes in the capital, 25 killed*". The original post turns out to be untrue as there had only been a scuffle at the local university football match, resulting in injuries and hospitalisation to a few students involved. However, the spiralling misinformation results in escalated tensions and full blown communal riots in the city. The TV anchor is likely to face legal sanction for disturbing public order. Is it appropriate to treat the 25,000 retweeters equally harshly?

Assessing the Legal Standard

At a high level, most legal systems liken Twitter posting to all other media broadcasting and the laws as applicable to newspapers, television and radio are readily applied. However, this causes significant regulatory dissonance because Twitter is not, in fact, functionally equivalent to these traditional media platforms.[19]

In the quest to establish the appropriate liability standard for retweets, the first task is the appropriate characterisation of the retweet. In function, a retweet can, in some respects, be

---

[18] Twitter tells its users: "You are responsible for your use of the Services, for any Content you post to the Services, and for any consequences thereof." *See* https://twitter.com/tos.

[19] Jacob E. Dean, *To Tweet or not to Tweet: Twitter, "Broadcasting," and Federal Rule of Criminal Procedure 53*, 79 U. CIN. L. REV. 769, 789 (2010).

analogised to a link to or quotation of another's posting[20] and, in others, to an independent and new publication. Thus far, the legal precedent has relied on the latter approach. For all intents and purposes, retweets have been treated like any other tweets regardless of the content first having originated from a third party. Looking at our two hypothetical cases from earlier in this article, this is not a satisfactory result. This is especially so in the social context surrounding instantaneous digital communication. The ensuing chilling effects on the act of sharing, itself an independent form of speech, have significant ramifications on the diversity of voices that can be heard and the sources they come from.

Simply put, are retweeters more like independent voices (i.e., through active publication) or are they better characterised as constituting a new category of intermediaries who facilitate third party access to original content (i.e., through linking)?[21] The questions become where on the continuum between liability for publication and linking should liability rest, and why? In searching for responses, the next section will demonstrate how the application of traditional media laws to tweeting and retweeting makes for a poor fit.

The Regulatory Framework

Commentators analogise tweeting to a stream of consciousness, like an electronic version of a coffee shop,[22] with the primary focus on frivolous conversation, gossip and minutiae.[23] Retweeting, even more so, falls into the category of non-serious social chatter of the nature of "do you know what XYZ said?" rather than formal, well-considered communication such as a news article or a segment on a television feature. Naturally, there is limited expectation of due diligence with respect to tweets and most users and viewers of Twitter content will likely be aware of the social context, informality and potential inaccuracies that characterise tweeting.

From a regulatory perspective, however, the key difference between Twitter and a coffee shop is that in the Twitterverse, potentially anyone in the world can play the role of either a permitted guest or an unintended eavesdropper. Speech, to which liability is most unlikely to attach in the real world, suddenly and unintentionally takes on a new character on social media although the digital speaker and the listener may not agree that they meant it to be any different in character.

---

[20] *See* Harbhajan Singh v. State of Punjab, (1961) CriLJ 710.

[21] *Supra* note 12, at 25.

[22] *Supra* note 14, at 36.

[23] Hannah Rogers Metcalfe, *Libel In The Blogosphere And Social Media Thoughts On Reaching Adolescence,* 5 CHARLESTON L. REV. 481, 499 (2010).

While social media platforms have a very different context from other news communication modes,[24] it does not mean that this can be a liability-free zone; such a result would be as inappropriate as legal overreach.

Whether an original tweeter or a retweeter, a Twitter user exposes himself or herself to the entire gamut of laws governing content and speech.[25] Both civil and criminal laws are used to curb and control online speech. Potential liability can take the shape not only of damages but also of fines and incarceration. Defamation, copyright infringement and public order laws stand out as prime examples of the heads of liability most commonly applied to online speech. The applicability of these laws to retweets will be the subject of the remainder of this article.

Defamation

For a claim of defamation to succeed the statement under consideration must be: (i) false, (ii) made about the aggrieved person's reputation or business, (iii) understood by a reasonable person to be of or concerning the aggrieved person, and (iv) made out to a third person.[26] With respect to public figures, in addition to the specified factors, there is a requirement to prove that the representation was precipitated by malice.[27] The principle of privilege permits certain professions with a degree of latitude in response to claims of defamation. For example, journalists are provided some latitude (qualified privilege) through the dilution of the 'truth' defence, in that they can resist a claim for defamation on the ground that the statement or publication is based on a reasonable verification of facts and that it was not produced with a reckless disregard for truth or precipitated by actual malice.[28]

While case law involving Twitter and defamation has been limited worldwide, of relevance to the Indian context is the case of *Chris Cairns v. Lalit Modi*.[29] This case related to a suit for defamation filed in the UK by New Zealand cricketer Chris Cairns arising out of the following tweet (since deleted) by former IPL Commissioner Lalit Modi: "*Chris Cairns removed from the IPL auction list due*

---

[24] *See*, for discussion of this issue, Rebecca Phillips, *Constitutional Protection for Nonmedia Defendants: Should There be a Distinction Between You and Larry King?*, 33 CAMPBELL L. REV. 173 (2010).

[25] *See* for a comprehensive list of Indian laws that might be applicable to content: http://copyright.lawmatters.in/2012/01/brief-compilation-of-indian-content-law.htm.

[26] Tata Sons Limited v. Greenpeace, I.A. No.9089/2010 in CS (OS) 1407/2010 (Delhi High Court) (India).

[27] *Id.;* R Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264.

[28] R. Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264 relying on New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

[29] *See* Chris Lance Cairns v Lalit Modi, [2012] EWHC 756 (QB).

to his past record in match fixing. This was done by the Governing Council today." The High Court ruled in favour of Cairns and quantified the damage to reputation as £75,000 with an aggravation of 20% due to sustained and aggressive assertion of the plea of justification insufficiently backed by evidence. In quantifying damages, the High Court noted that the tweet was received by a limited number of followers that the parties agreed to be 65. Modi, thereafter, appealed to the Court of Appeal against the order of the High Court on the issue of quantification of damages.[30] On appeal, the issue in question concerned the appropriateness of the damages in light of the tweet's limited publication (both time and audience). In relation to this issue, the Court of Appeal recognised that damages for defamation should not be restricted or limited to the original recipients of a publication, and that the court must consider their likelihood to percolate through the Internet.[31] The Court of Appeal added that the issue of percolation is of particular relevance and 'immeasurably enhanced' due to the emergence and ease of availability of the World Wide Web.[32]

With respect to the re-publication of defamatory content, Indian courts have accepted that any such re-publication will give rise to a new action for defamation.[33] The re-publisher is required to defend the publication on the same grounds as available to the originator, i.e., by proving that the elements of defamation have not been made out. There is no defence of due diligence reporting or fair comment readily available. The underlying basis of this treatment is the position that the re-tweet constitutes an action of independent speech relaying information afresh, possibly to a new and different audience than the original tweet.[34] The retweeter is considered a principal actor rather than as an intermediary enabling content to be relayed to others.

Unlike a simple link to a website (which may contain infringing content) the retweet is not content-neutral. It conveys the allegedly infringing content fully and without reference (other than attribution of authorship) to the original posting. The retweet itself may be all there is, with there being no reason for a viewer of the contents to access the original tweet to view its contents. The case could therefore be made that the repetition and amplification of the content is in and of itself fair basis for attributing re-publication liability.

---

[30] *See* Lalit Modi v. Chris Lance Cairns, [2012] EWCA Civ 1382.

[31] Termed the 'grape-vine effect' *see* Crampton v Nugawela [1996] NSWSC 651.

[32] *Supra* note 30.

[33] Harbhajan Singh v. State of Punjab, (1961) CriLJ 710; In Re: E.V.K. Sampath, AIR 1961 Mad 318. It should also be noted that in Watkins v. Hall, 1868 (3) QB 396, the Queen's Bench suggested that repetition of a slanderous statement grants it greater weight and may result in greater injury to the person affected.

[34] *Supra* note 12 at 7.

That said, there are compelling reasons why all tweets, not just retweets, ought to be treated differently from those acts of publication forming part of the traditional media industry. The defamation law is grounded in the premise of a mismatch in size, resources and reach between the publisher of content and the subject matter of the defamatory publication. In large part, the availability of the remedy of defamation and the role of a public trial is to set right an unequal balance between the large publisher (with access to a professional editorial and legal team and wide circulation) and the relatively powerless individual who might not have ready access to a similar scale of resources or reach.[35] With Twitter, this is no longer the case. Though it might not be simple, for a nominal cost it is possible for the subject of the tweet to reach potentially the same audience that the original poster had in order to refute, clarify and respond[36] in more or less real-time. The original poster also has the opportunity to undo damages by reformulating, retracting and relaying[37] information he or she realises is inaccurate or illegal without having to wait for the completion of an entire passive news cycle, as would be the case with traditional media.[38] The opportunity here is to fight bad speech with more and better speech[39] relayed to potentially the same audience and on the same platform and scale. Where effective remedies and solutions of this sort are available and the defamation defendants are not necessarily in positions of mismatched power and reach, it may be strongly argued that the defamation law must find a new balance.

Copyright

Under the Copyright Act, 1957, infringement of a copyrighted work consists of two essential elements:[40]

(i) There must be sufficient objective similarity between the infringing work and the copyright work; and

(ii) The infringing work must have been derived from the copyright work.

There are certain "affirmative defences" available to a defendant in the case of an allegation of copyright infringement. These exceptions include "fair dealing", which covers private use, research

---

35 *Supra* note 14 at 7.

36 *Supra* note 14 at 18.

37 *Supra* note 15 at 9.

38 *Supra* note 14 at 55.

39 *Supra* note 11 at 36.

40 Sulamangalam R. Jayalakshmi v. Meta Musicals, 2001 (1) Raj.150.

work, review, criticism, etc. and "reporting of current events", which constitutes reports of works in the various forms of publication."[41]

With respect to whether original tweets are copyrightable and if retweets might amount to infringement of these tweets, the copyright law generally has a minimum threshold of length for originality that tweets might not satisfy.[42] Moreover, there is arguably an implied license from tweeters to third parties willing to retweet their content, with certain types of retweets also possibly qualifying as commentary and news reporting and, therefore, amounting to fair dealing.[43]

The issue of relevance is not whether the retweeter might infringe the copyright in the original tweet but it is whether a retweeter can be responsible, as the original tweeter might be, if the tweet links to, makes available or otherwise distributes copyright infringing content owned by third parties. A typical example is of a tweet providing a link to a file locker enabling the free download of an illegal copy of a new movie.

While there is only limited Indian case law on the appropriate liability standard for linking to copyright infringing content, internationally the standard is somewhat clearer. Providing links to copyright infringing content may not always constitute a primary infringement,[44] though it can certainly render the person providing the links liable for secondary infringement (for facilitating or inducing the principal offence).[45] Liability of either sort is unlikely to attach unless it can be proved that the linker was actively encouraging or inducing infringement, had reason to know that the content was infringing, or had actual and specific knowledge of its infringing nature.[46] Linking to other types of infringing content can also give rise to liability when the action is undertaken to evade a court order, to promote illegal conduct by others[47] or when there is complicity with the

---

[41] §52 of the Copyright Act, 1957.

[42] Stephanie Teebagy North, *Twitteright: Finding Protection in 140 Characters or Less*, 11 J. HIGH TECH. L. 333, 4 (2011).

[43] Adam S. Nelson, *Tweet Me Fairly: Finding Attribution Rights Through Fair Use in the Twittersphere*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 697, 15 (2012).

[44] *See,* for reference, Ticketmaster Corp. v. Tickets.com, 248 F.3d 1173 (9th Cir. 2001).

[45] *See,* for reference, Cooper v. Universal Music Australia Pty. Ltd. [2006] FCAFC 187; Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290 (D. Utah 1999).

[46] *See* Mark Sableman, *Link Law Revisited: Internet Linking Law at Five Years,* 16 BERKELEY TECH. L.J. 3, 1273 (2001).

[47] *Id.*

original poster to commit an offence.[48] Upon careful evaluation of the nature of a retweet, these principles are potentially equally applicable to retweets.

Public Order Offences

Section 66A of the Information Technology Act, 2000 ("**IT Act**") was inserted vide the Information Technology (Amendment) Act, 2008 and created a new criminal offence.[49]

Of direct relevance to retweeting liability are sub-sections (a) and (b) of Section 66A. Sub-section (a) deals with the sending of any information that is 'grossly offensive' or 'menacing' in character**.** The terms 'grossly offensive' and 'menacing' have not been defined in the IT Act and, thus far, there has been no meaningful judicial evaluation of what might be considered to be 'grossly offensive' or 'menacing'. This offence is seemingly set up as a strict liability offence with no *mens rea* or knowledge component required. Sub-section (b) has three essential conditions to be met for an offence to be established: (i) the knowledge of the sender, (ii) the persistent sending of electronic messages, and (iii) the purpose of the messages.

With respect to applicability to tweets and retweets, it is evident that the phraseology of Section 66A of the IT Act is so wide that it includes within its ambit almost all forms of online speech and expression. Importantly, no distinction is made between original postings (tweets) and shares or reposts (retweets).

There have been several instances over the last year of Section 66A of the IT Act being used in response to online speech on social media platforms.[50] A recurring theme in each of these cases is

---

[48] Alain Strowel & Nicholas Ide, *Liability with Regard to Hyperlinks,* 24 COLUM-VLA J.L. & ARTS 403, 444 (2000).

[49] §66A deals with "Punishment for sending offensive messages through communication services, etc." and states:

"Any person who sends, by means of a computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character;

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message."

[50] In April 2012, Ambikesh Mahapatra, a professor of chemistry from Jadavpur University in West Bengal was arrested for emailing a caricature of West Bengal Chief Minister Mamata Banerjee to his friend. In May

that those charged under Section 66A had made or interacted with posts or transmitted messages relating to politicians or the kin of politicians. The increasing frequency of these cases led to the filing of a petition in the Supreme Court of India challenging the legality and constitutionality of Section 66A on the basis that it is so wide and vague and incapable of being judged on objective standards, that it is susceptible to "wanton abuse and hence falls foul of Article 14, 19(1)(a) and Article 21 of the Constitution."[51] Subsequent to the filing of this petition and the public outrage ensuing from the repeated incidents, the Government of India issued fresh interim guidelines in the form of an advisory,[52] stating that a police officer no less than the rank of District Commissioner of Police DCP can sanction prosecution under Section 66A. In metropolitan cities, such an approval would have to be given by officers at the level of Inspector General of Police (IGP). Only officers of these ranks will be allowed to permit registration of a case for offences under the IT Act relating to spreading hatred through electronic messages in a bid to prevent the misuse of the legislation.[53] These procedural safeguards notwithstanding, there is still a lack of clarity at the administrative and judicial levels on the substantive ambit of the offences, when and how they must be applied and appropriate limitations, exceptions and defences.

Of direct relevance to the Twitter liability standards debate on public order offences are the 'Interim Guidelines on prosecuting cases involving communications sent via social media' (the "**Guidelines**") issued by the United Kingdom's (the "**UK**") Crown Prosecution Service by the

---

2012, two Air India employees, V. Jaganatharao and Mayank Sharma, were booked by the Mumbai Police for allegedly uploading lascivious and defamatory content on Facebook and Orkut against a local politician and for threatening him with death while insulting the national flag in the process. In October 2012, businessman Ravi Srinivasan was arrested and charged under Section 66A of the IT Act by the Puducherry Police for having made an allegedly false accusation on the finances (the tweet stated: "got reports that Karti chidambaram has amassed more wealth than vadra.") of Karti Chidambaram, the son of the Union Finance Minister P. Chidambaram. In November 2012, two young women from Palghar in Mumbai, Maharashtra were arrested and booked under Section 295 (A) of the Indian Penal Code which deals with the "outraging of religious feelings of any class" and Section 66A of the IT Act. While one of the girls was booked as a result of posting a comment on Facebook against the shutdown in Mumbai after the death of Bal Thackeray, her co-accused was arrested for 'liking' the said comment on Facebook. In February 2013, the head of the Mahila Congress in Kerala Bindu Krishna filed a defamation case against a Facebook poster as well as over 140 people who shared the post in relation to the alleged role of the Rajya Sabha Deputy Chairman P.J. Kurien in the infamous Suryanelli rape case.

[51] *SC accepts PIL challenging Section 66A of IT Act, November 29, 2012*, *available at* http://articles.timesofindia.indiatimes.com/2012-11-29/india/35433946_1_cognizable-offence-section-66a-shreya.

[52] *Govt modifies Sec 66(A) of IT Act after recent Facebook controversies, November 29, 2012, available at* http://ibnlive.in.com/news/govt-modifies-sec-66a-of-it-act-after-recent-facebook-controversies/307991-3.html

[53] Advisory on Implementation of Section 66A of the Information Technology Act, 2000, (No. 11(6)/2012 – CLFE), January 9, 2013, *available at* http://deity.gov.in/sites/upload_files/dit/files/Advisoryonsection.pdf.

Director of Public Prosecutions ("**DPP**") that came into immediate effect on December 19, 2012. They were issued amongst growing concerns in the UK over the proportionality of prosecutions for offences committed on social media following the case of *Chambers* v. *DPP*.[54] Importantly, these Guidelines apply equally to the resending (or re-posting/retweeting) of communications.[55]

According to the Guidelines, any prosecution of social media offences must pass two tests:

(i) *The test of evidential sufficiency*[56] which means 'that an objective, impartial and reasonable jury (or bench of magistrates or judge sitting alone), properly directed and acting in accordance with the law, is more likely than not to convict'; and

(ii) *The test of public interest*[57], which means that the prosecution is the interests of the general public.

The Guidelines identify the following three specific categories of cases that will be 'prosecuted robustly'.[58]

(i) Communications which may constitute credible threats of violence to persons or damage to property;[59]
(ii) Messages which specifically target an individual or group of individuals and which may constitute harassment or stalking or which may constitute other offences such as blackmail;[60] and
(iii) Communications which may amount to a breach of a court order.[61]

[54] [2012] EWHC 2157. This involved Paul Chambers' conviction for sending a 'menacing' tweet threatening to blow up the Robin Hood Airport in South Yorkshire, which was overturned on appeal.

[55] ¶ 2.

[56] ¶5.

[57] ¶5.

[58] ¶13.

[59] ¶12(1).

[60] ¶12(2).

[61] ¶12(3).

A fourth category of cases is mentioned as being subject to a higher threshold, on the premise that in many cases, prosecution of cases of this nature is unlikely to be in public interest:[62]

(iv) Communications which do not fall into any of the above categories and fall to be considered separately, i.e., those which may be considered 'grossly offensive', 'indecent', 'obscene' or 'false', under Section 1 of the Malicious Communications Act 1988 or Section 127 the Communications Act 2003.[63]

In this fourth category of cases a prosecution may only be brought under where the communication is 'more than':

(i) Offensive, shocking or disturbing; or

(ii) Satirical, iconoclastic or rude comment; or

(iii) The expression of unpopular or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it.[64]

The Guidelines also list various factors that must be considered in deciding whether a prosecution is in public interest, *inter alia*, stating that a prosecution is unlikely to be necessary and proportionate where:

(i) The individual has taken swift action to remove the communication or expressed genuine remorse;

(ii) Swift and effective action has been taken by others, for example, service providers, to remove the communication or block access to it;

(iii)The communication was not intended or obviously likely to reach a wide audience, particularly where the intended audience did not include the victim or target of the communication; or

[62] ¶13.

[63] ¶12(4).

[64] ¶36.

(iv) The content of the communication did not obviously go beyond what could conceivably be tolerable or acceptable in an open and diverse society which upholds and respects freedom of expression.[65]

The Guidelines emphasise the unique context of social media communications and draw a distinction between social media communications and normal communications, stating that 'prosecutors should have regard to the fact that the context in which interactive social media dialogue takes place is quite different to the context in which other communications take place. Access is ubiquitous and instantaneous. Communications intended for a few may reach millions.'[66] The Guidelines also caution that 'particular care' should be taken when using public order offences to prosecute social media cases, since public order legislation is primarily concerned with words or actions carried out in the presence/hearing of the accused.[67] Further, prosecuting a minor is seen as 'rarely likely to be in the public interest' according to the Guidelines, on the basis that children and young persons may not fully appreciate the potential harm and seriousness of their communications.[68]

The Guidelines are the first significant intervention that has rationalised social media legal standards. It cautions that the laws with respect to public order and threats must be applied carefully and sparingly in the context of social media, especially when the person posting the content is not actively inciting, harassing or offending a person or persons in his or her physical proximity or otherwise potentially under his or her influence. Merely because a social media post is capable of being viewed by *every* member of the public does not mean that it is actionable if *any* member of the public could potentially be incited, harassed or offended by it. What must be avoided at all costs is the 'heckler's veto'.[69]

Beating a Retreat on Liability

Functionally, a retweet is not very different from a hyperlink that informs the viewer of the existence of the original tweet. Take our two hypothetical cases, for instance. In Case A, retweeters are repeating a statement made by a public figure and, in Case B, the statement of a respect journalist. Speaking about it to friends over dinner or for that matter quoting the tweet to a large

---

[65] ¶ 39.

[66] ¶ 35.

[67] ¶ 42.

[68] ¶ 41.

[69] Lyrissa Barnett Lidsky, *Incendiary Speech and Social Media,* 44 TEX. TECH. L. REV. 147, 9 (2011).

gathering is most unlikely to result in any liability whatsoever. Why should this be any different in the digital context when shared with followers?

A retweet refers factually to an independently existing and verifiable event that has already occurred, i.e., the posting of the original tweet by another user. The viewer of this retweet, by clicking on the retweet or the original poster's handle or profile name, can independently refer to and confirm the authenticity of the original tweet. This feature makes retweeting significantly different from a cross-platform re-publication. While the actual audience might have been amplified to some extent, the potential audience never is – after all, with all tweets being public by default, any follower of the retweeter has equivalent access to the original tweeter. The liability for original tweets is premised on the fact that a tweet is publicly accessible by *anyone* on Twitter. When evaluating the liability standard for retweets the question then is whether it is appropriate to claim that new viewership is harnessed by the retweet? Is there indeed a new act of 'publication' when the original tweet has already been published in a manner accessible to anyone who can view the retweet?

In the context of public order offences, the principles established by the UK Guidelines take the implementation of the law in the right direction. If implemented in the spirit of the Guidelines, public order offence laws cannot legitimately be applied to retweets in the same manner as they are to original tweets. Although retweets can magnify the risk of violence[70] and their immediacy give little time for evil counsels to be countered by good ones,[71] their increased remoteness from the mischief sought to be protected against must be equally kept in mind. This is not to say that retweets cannot amount to public order offences, but certainly the circumstances would be rare and exceptional, where the public interest not only trumps the freedom of speech of the retweeter and the right of the public to receive the retweet. Advocacy must also effectively be differentiated from incitement.[72]

To summarise, in the valuable quest to protect the end-to-end character of the internet, the law must recognise and protect a new breed of internet intermediaries – the content sharers.

Safe Harbours

With new technologies often come predictions of dire technological harm. Failure to regulate is projected as the most risky proposition and plaintive cries are made for new legal controls. As we

[70] *Id.,* at 13.

[71] *Supra* note 69 at 14.

[72] *Supra* note 69 at 18.

have seen, in particular with Section 66A of the IT Act, legislating when a technology appears new and mysterious can result in questionable laws and judicial precedents.

On balance, the public's interest is better served in almost every instance with access to more information from more sources as opposed to less. For this reason alone, the refraction and sharing of digital speech must find legal protection. Viewers of social media messages, a constituency that significantly overlaps with those posting on these platforms, are aware of the social context in which they post messages on social media and the resulting limitations.[73] They know that not only are editorial filters less robust but that there is an overall reduced degree of discipline in this mode of communication. This gives them reason to automatically filter and evaluate the accuracy and authenticity of the information posted, acting with a general cynicism that they would not generally display towards traditional media. Any legal standard that fails to understand this is unlikely to promote the public interest. In essence, there are good reasons to treat a retweet as we would an act of quotation, attribution or a statement of a pre-existing fact. There are equally good reasons to treat a retweeter on par with a traditional internet intermediary.[74] Limiting speech often has the opposite effect to the intended and runs the risk of giving bad speech a mystique and making it seem more desirable.[75] By protecting the dissemination and distribution of speech through safe harbours from liability for those facilitating this through social media sharing, an overarching public interest is served.

Principles of Liability for Retweets

Based on what has gone above, the following principles are recommended as necessary elements of a legal framework for attributing liability to the retweeting of illegal and infringing content:

(i) Fundamentally, the law should treat a retweet on par with a linked quotation rather than a fresh publication. It must recognise the retweeter as a new category of digital intermediary, deserving of protection of a limited nature. This characterisation would

---

[73] *Supra* note 15 at 9.

[74] §2(1)(w) of the IT Act states that an "intermediary" with respect to any particular electronic message means 'any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message'. This definition recognises the existence of independent pre-existing information which is being transmitted 'on behalf of another'. While retweeting is not necessarily done at the instance of or upon the request of the original poster and fellow users have not been traditionally recognised as intermediaries, a number of the principal elements of this definition are satisfied equally by an intermediary user such as a retweeter as it is by traditional intermediaries such as ISP, web-hosts, search engines and other similar services.

[75] *Supra* note 14 at 50.

not absolve the retweeter of all liability but would necessarily isolate and pre-determine the types of situations in which a retweeter might encounter liability.

(ii) Liability may attach to a retweet only in exceptional circumstances and should primarily be limited to specific situations, *inter alia*, where it can be conclusively established that the retweeter:

(A) knew of the defamatory, infringing or illegal nature of the content and retweeted it regardless; or

(B) demonstrated gross negligence in failing to verify the veracity or legality of the content in the face of reasonable doubt and retweeted it regardless; or

(C) was complicit with the original poster of illegal or infringing content and retweeted the said content in furtherance of this complicity; or

(D) retweeted content knowing that this would violate a court order prohibiting its publication or distribution; or

(E) after being put on notice of the illegality or infringing nature of the original tweet, intentionally failed or refused to delete the retweet and/or issue a retraction or clarification on the same platform in an expeditious manner; or

(F) retweeted content in an intentional attempt to incite hatred or an offence or to systematically and repeatedly harass an individual.

(iii) Retweeters must in all circumstance be able to enjoy the defences and privileges that the original poster does. For example, if the original post is from an established news source and the original poster enjoys journalistic privilege, so should the retweeter. This would ensure that there is never a case when a retweeter is held liable for content for which the original tweeter is not. Any other theory of defence that relies on the position, profession or activity of the poster rather than the nature of the content must be equally accessible to the retweeter. This, along with the liability principles enunciated above, will enable users to retweet content from established news sources and journalists without having to take on risks that the original posters do not.

This Article postulates that a legal framework incorporating these principles – perhaps through relevant amendments to the IT Act – will help foster an information environment in which protecting the diversity of sources combines effectively with responsible content distribution. This is a balance worth finding with immediacy and the time has come for the law, as it stands, to beat a retreat.

BOOK REVIEW: "OVERLAPPING INTELLECTUAL PROPERTY RIGHTS" BY NEIL WILKOF AND SHAMNAD BASHEER (eds.)

V. Lakshmi Kumaran[*]

Book details:
Title: Overlapping Intellectual Property Rights
Edited by: Neil Wilkof and Shamnad Basheer
Publisher: Oxford University Press (2012)
Pages: 521

Introduction

The Intellectual Property laws have a foundation, as many believe, in John Locke's labour theory of property and broadly recognise the need to protect the fruits of one's intellectual labour. The creative nature of the human mind has no contours but, while the human tendency to compartmentalize and segregate subject matter does help in making things simpler, it may not always the case. Many creative minds are free from the fetters of classification and 'compartmentalisation' and may create something that could be subject matter of more than one 'IP regime'.

Moreover, with the advent of complex technologies which have applications in multiple sciences, the lines between distinct disciplines like engineering, art and life sciences, can be seen to be diminishing. This raises several questions for the stakeholders. Can a plant variety or parts thereof, be offered protection under both plant variety and patent law? If yes, which one should the individual choose and what should be the considerations involved when choosing one over the other? What do the UPOV Convention and TRIPS agreement have to say about this? Similarly, a product may be covered by Design protection law as well as Patent law, covering the functionality attached to the design itself. Is there interplay between right to publicity and trademark law? Are there overlaps in the moral and economic rights of authors over their works? How complex is the

[*] Managing Partner, Lakshmi Kumaran & Sridharan, Attorneys, B-6/10, Safdarjung Enclave, New Delhi-110029.

relationship between Patents and Utility Models? These and many more are very contemporary issues which need to be addressed.

About the Book

The book ***Overlapping Intellectual Property Rights,*** edited by Neil Wilkof and Shamnad Basheer, seeks to give answers to these issues or,at least, offers comprehensive insight into the issues and stakes and is therefore an invaluable addition to the existing literature on Intellectual Property Law. The legal context given to these questions of overlap is from the perspective of US and English law with inferences drawn from the EU as well. Although, it may seem as a limitation, it only provides for uniformity in the analysis and readers have, at their disposal, what can be described as comprehensive chart at the end of the book that contains snippets on the overlapping IPR regimes in 17 countries. The size of the five hundred page book does not do justice to the spectacular labour of several authors that has gone into creation of this work which has a vast reach in terms of number of fields and jurisdictions. A perusal of the "list of contributors' would show that the authors of different chapters are from diverse background such as leading universities, research institutes, and prominent law firms from different parts of the world such as USA, UK, Singapore, Australia, India, Belgium etc. This lets the reader have a wider perspective over the underlying theme.

The theme itself is intriguing and is something that has, at one point or the other, caught the imagination of many academicians, students and professionals, but a comprehensive work such as this is not common. The book follows a unique pattern while discussing an issue and this is what makes it much more interesting to read than other traditional works in the same field. Going by its theme, a perusal of the index would show the reader the huge canvas on which multiple authors have written about overlapping IPRs.

The chapters in the book have been organized in clusters so as to allow the reader to grasp all the possible overlaps which can take place while considering one particular IP law. While most works introduce the concept first and proceed with the practical applications thereafter, this book follows the opposite methodology. Each chapter begins with a hypothetical and practical fact situation, which introduces the reader to the various intricacies of IP law which can originate from a single

creation. More often than not, these hypothetical fact situations are based on real cases; *See Franek v. Franco* in the overlap between patents and design and *Theberge v Galeri d'Artu Petit Champlain* concerning the correlation between moral rights and economic rights. The hypothetical fact situation therefore, forces the reader to think and introspect, about the possible solutions to the problem. The fact situation serves as a spring board for the imagination of the reader to appreciate the theme of every chapter of the book i.e. overlap of the specific intellectual property rights.

After a thorough evaluation of the relevant provisions of law and the overlaps between the same, the authors give a complete analysis of the hypothetical fact situation. Finally, each chapter of the book concludes with a summary of the contradictions/similarities between the laws in various jurisdictions and the best course of action if and when a similar overlap does take place. Hence, the book touches upon a multidisciplinary area of law, which was yet to be properly explored and analyzed, and it deserves critical appraisal for the same.

Brief highlights on some of the chapters will enable any prospective reader to get an idea of the extensive and interesting nature of the work. Through 17 chapters, one can see the sheer brilliance in the exceptional work of the authors in covering the most prominent and complex overlaps in intellectual property rights. An example is the overlap between design protection and patent protection wherein the position of law varies considerably across jurisdictions. For instance, if the technical advantage in the concerned creation trumps the presence of eye appeal, then design protection may be refused in the US. The sensitive interplay between breeder's rights and patents, particularly, the conflict between farm saved seed vis-à-vis patentee's rights over the plant, have also been deliberated upon. The book also takes the reader through more contemporary issues with regard to the relationship between trademark rights and unfair competition, such as 'slavish imitation' and comparative advertising. Further, the book sheds light on the design vis-à-vis copyright debate wherein, laws in various jurisdictions expressly prohibit an overlap between the two, however the definitions of the subject matter being governed by the two laws are not clear and this is the reason behind the ensuing confusion. The book also analyses the overlap between domain names and trademarks. After providing an interesting history of how the relationship between the two regimes has developed, practical solutions have been offered that may be very useful for practitioners, especially the US. Similarly, the book offers an extensive discussion on interplay

between publicity rights and trademark law. While both may seem to have some similarity insofar as they relate to asserting the right to unique name and image, both are distinct when it comes to enforcement, the former enforced by showing unauthorized usurping of commercial benefit from a person, the latter is enforced by showing likelihood of confusion. Moreover, the book, in its last chapter, attempts to harmonise the stand between, intellectual property rights and competition rules which traditionally, have been viewed to be in conflict with each other.

The book explains the individual concepts very clearly, thereby enabling the reader to have a better perspective over the instances where overlaps can occur. As mentioned already, the book gives an overview of the position of law on the specific overlapping IP rights in multiple jurisdictions, particularly, the United States, the United Kingdom, the European Union, along with a chapter dedicated to India. Where necessary, the book also highlights the provisions of law in other jurisdictions so as to give a holistic understanding of the discrepancies which exist in the laws across jurisdictions when considering the same issue.

The India chapter

A special mention is imperative for this chapter on the Indian perspective, written by no less a person than Prof. Shamnad Basheer, the First Ministry of Human Resource Development Chair Professor in IP Law at WB National University of Judicial Sciences. This Chapter traces the doubling of the number of IP over the years and then goes on to examine the common underlying thread that runs through these categories of IP. It begins with the classic example of complete software – whether it is a literary work entitled to copyright protection and/or also to patent protection. The article very aptly examines the issue of overlapping of IPs by noting the two extreme positions – only single IP or multiple protections. At the same time, he also highlights the fact that the perceived overlap may not be overlap at all. While copyright on software, for example, protects the actual expression of the source code, the patent may protect the underlying idea / functionality. Thereafter, he goes on to examine overlap of IP in India. The overlap between patents and copyrights, patents and trademarks, copyright ts and trademarks, copyright and trade secrets, copy rights and designs, trade marks and G.I., etc., are discussed in detail. The Chapter concludes with the decision in *Microlube* case, which has been referred to a large bench of the Delhi High Court, to

see if Judges will lay down a doctrine of preclusion or prune down the scope of specific IP regimes to avoid overlap.

The larger bench has now decided the issue (May 15, 2013) wherein the majority opinion, delivered by Justice Shakdher, states that passing off remedy will be available to a person with respect to a design already registered under the Designs Act, 2000. However, Justice Manmohan Singh has differed and cautioned that passing off remedy is not available for those features/aspects of the design which are covered under the novelty of the registered design, even after the expiry of the registration. Other aspects of passing off, as per Justice Singh, like trade dress etc. are open for challenge so long as they do not conflict with the registered design under the 2000 Act.

Concluding thoughts

The book would have a good impact in stimulating professional legal minds on such 'juicy' issues that they would, if not already seen, surely see in courts sometime soon. At the same time, it would be of great help in introducing students to such advanced concepts of overlapping IPRs and to fields such as publicity rights and unfair competition law, which usually may not form a part of the regular IP law curricula. Although the book was written by authors from various countries and varied fields, it presents a remarkably coherent style of writing. It would certainly help professionals in appreciating that, irrespective of jurisdictions, the core issues arising out of overlap may be very similar. At the same time, practitioners would also find that questions on overlap may appear very simple at the outset, but they are indeed much complex when one goes deeper in the fact situation. The wide array of recent cases which have been included in the book, would also enable the reader to appreciate the current position of law. Needless to say, lawyers from all over the world would also benefit from this scholarly work, since it focuses on contemporary issues which may arise while practicing law in the IP sector. For any experienced practitioner it would not be difficult to contemplate such interesting overlaps and thus, find this book valuable, especially in competitive and developing countries like India where IP laws such as trademark and copyright law have significant number of precedents, whereas laws relating to Patents, plant variety, competition law etc. are still at a nascent stage. In the circumstance that a particular creation can be protected under multiple IP laws, it becomes essential for a lawyer to work out the best mode of protecting the

concerned creation. Overall, the Book is a veritable feast to practitioners and academics in the IP field.

Lastly, it would be interesting to see the additions and supplements which the authors would make in the subsequent editions of this book.. Some IP regimes like copyright are so diverse that it may be pertinent to discuss scenarios of such overlap within different forms of copyrightable works such as musical work, sound recording or performance which would be interesting to see because nature and extent of protection may vary for different kinds of works under Copyright law. Moreover, although not an overlap per se, intellectual property rights do have close relationship with some regulatory obligations. One of them has been discussed in the chapter dealing with Patents and Regulatory data exclusivity. However, there are other interesting subjects that may be looked at such as obligations arising out of biodiversity concerns which have a significant impact on research, patents or plant variety protection. Needless to say, study of overlaps is crucial as overlaps in intellectual property rights, are only set to increase in the future

GIVE ME MY SPACE AND TAKE DOWN HIS

Ananth Padmanabhan[*]

The Copyright (Amendment) Act, 2012 has introduced fair use provisions to exempt intermediaries from liability in certain specific situations and provides them an opportunity to take down infringing content when brought to their notice. Lawmakers in India have certainly taken a positive step forward, and the above provisions on a plain reading, seem to protect and nurture a file-sharing business model that offers immense possibilities for the future, even at this nascent stage. However, the judicial response to this Parliamentary intent is a matter of serious concern, considering the recent pronouncements of the Delhi High Court in the Myspace case and the decision of the Madras High Court in the R.K. Productions case. The amendments also have to be viewed in light of the widely worded John Doe orders issued by Indian Courts, which pose a potential risk to the growth of the file-sharing industry and the possibility of a chilling effect on free expression and dissemination of information.

In this paper, the author examines the content of the amendment and the nuances in its language, the manner in which it could be interpreted by Courts and the extent to which this amendment could foster the growth of the file-sharing and streaming industry. To do this, the issue of intermediary liability in Indian law prior to the amendment has been examined. The paper also briefly studies the legal position on intermediary liability in the United Kingdom as discussed in the Newzbin2 case and examines whether the post-amendment provisions in India are open to similar interpretation and application.

TRANSIENT 'AND' INCIDENTAL: OR SHOULD IT BE AN 'OR'?

In 2010, the controversial Copyright (Amendment) Bill came up for deliberation before the Parliamentary Standing Committee on Human Resource Development, headed by Mr. Oscar Fernandes. While a major part of the discussion revolved around the altered royalty structure and rights allocation between music composers and lyricists on one hand, and film producers on the other, it can be safely stated that this is the most significant amendment to the Copyright Act, 1957 beyond this reason alone. The amendment seeks to reform the Copyright Board, bring in a scheme of statutory licenses, expand the scope of performers' rights and introduce anti-circumvention measures to check copyright piracy. As part of its ambitious objective, the amendment also attempts to create a new fair use model to protect intermediaries and file-sharing websites.

The Copyright (Amendment) Act, 2012, which gives expression to this fair use model through Sections 52(1)(b) and (c), reads thus:

---

[*] Advocate, Madras High Court and author of INTELLECTUAL PROPERTY RIGHTS: INFRINGEMENT AND REMEDIES (2012). Disclosure: The author, in his capacity as counsel for the South India Music Companies Association, has represented provisions in respect of the subject matter before the Parliamentary Sub-Committee on the Copyright (Amendment) Bill, 2010.

52. Certain acts not to be infringement of copyright. – *(1) The following acts shall not constitute an infringement of copyright, namely:*

*(a) to (ad) – ******

(b) the transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public;

(c) transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder, unless the person responsible is aware or has reasonable grounds for believing that such storage is of an infringing copy:

Provided that if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work, complaining that such transient or incidental storage is an infringement, such person responsible for the storage shall refrain from facilitating such access for a period of twenty-one days or till he receives an order from the competent court refraining from facilitating access and in case no such order is received before the expiry of such period of twenty-one days, he may continue to provide the facility of such access.[1]

From a plain reading, it is clear that two important exceptions are carved out: *first*, in respect of the technical process of electronic transmission, and *second*, in respect of providing electronic links, access or integration. The discussion on this provision by the Parliamentary Standing Committee, and the representations made before this Committee by various stakeholders have been recorded in the Standing Committee Report[2] and merit attention. The Human Resources Department, in its submission, made it clear that the purpose behind clause (b) was only to exempt liability arising out of 'caching', in tandem with international practice. Therefore, any *deliberate* storing of the works would still amount to infringement. Similarly, the Department contended that clause (c) only sought to carve out a safe harbour exemption for internet service providers.

Content providers such as Saregama RPG Enterprises, the Indian Motion Picture Producers Association, the Indian Music Industry and the South India Music Companies Association cried wolf and placed on record their concern that such a fair use model would certainly end up being abused. The specific worries were that even illegal downloaders and suppliers of copyrighted

---

[1] Indian Copyright Act, 1957, § 52.

[2] DEP'T-RELATED PARLIAMENTARY STANDING COMM. ON HUMAN RES. DEV., TWO HUNDRED TWENTY-SEVENTH REPORT ON THE COPYRIGHT (AMENDMENT) BILL, 2010 (2010), *available at* http://copyright.gov.in/Documents/227-Copyrightamendment.pdf .

content would rely upon this provision to plead that their storage was incidentally made, in the process of transmission, and that these provisions cast an additional burden on content providers to specifically request the take down of each infringing file – a task virtually impossible in the case of online piracy. The Business Software Alliance also lent their support to these stakeholders by submitting that the initially prescribed period of fourteen days, given to the content providers to obtain a judicial order to ensure the continued restriction on access to the infringing content, was too short a period.

On the other hand, intermediaries and online service providers were critical of the proposed provisions which, in their opinion, did precious little to safeguard their interests. Ebay India proposed that the words "transient and incidental", as found in the Bill, should be substituted with "transient or incidental". Yahoo India incisively analysed the wording of the Bill and submitted that the loose language employed therein could result in problems while carrying out various operations such as search, hosting, information retrieval and caching. A specific request was placed to amend the Act to provide clearly that an internet service provider would be liable only if it: (i) had knowledge of the infringing activity, and despite such knowledge, failed to remove the infringing content, or (ii) induced, caused or materially contributed to the infringing conduct of another. The Standing Committee accepted some of the above suggestions and recommended that the fourteen day period may be reviewed in order to achieve a more harmonious balance between the rights of content owners and that of a service provider to do business. This later translated into the twenty-one day window, as currently seen in Section 52(1)(c). The Standing Committee also accepted Ebay India's proposal to substitute the expression "transient and incidental" with the expression "transient or incidental". However, no heed was paid to the submissions made by Yahoo India pertaining to the inherent ambiguity in the language employed in Section 52(1)(c), and this is precisely where the amendments could actually falter in achieving their stated objective.

Infringement: Of Primary and Secondary

The conceptual issue that lies at the heart of the debate on fair use exemption for intermediaries is one of liability. Liability for copyright infringement can either be primary or secondary in nature. Primary liability, such as the case of a file-sharer *deliberately* storing or facilitating the transmission of infringing works to the public, is in any case not covered within the purview of the fair use exceptions introduced. It is only secondary liability, where the primary infringer is provided with a space that can be used as a conduit pipe, channel or network to transmit illegal copies created by him, that forms the subject matter of the newly introduced fair use model. Hence, it is imperative

to understand the difficulty faced, even by Courts, while adjudicating on the permissible limits of activity that facilitates, or could potentially facilitate, copyright infringement.

The classic divide on this issue is reflected in two judicial pronouncements – separated by a gap of more than two decades – delivered by the U.S. Supreme Court. In *Sony Corporation v. Universal City Studios Inc.*,[3] popularly known as the *Betamax* case, the U.S. Supreme Court held that the manufacturers of home video recording devices, known in the market as Betamax, would not be liable to copyright owners for secondary infringement since the technology was capable of substantially non-infringing and legitimate purposes. The U.S. Supreme Court even observed that such time-shifting devices would actually enhance television viewership and therefore find favour with a majority of copyright holders as well. The majority did concede however, that in an appropriate situation, liability for secondary infringement of copyright could well arise. In the words of the Court, "*vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another*." However, if vicarious liability had to be imposed on the manufactures of the time-shifting devices, it had to rest on the fact that they sold equipment with constructive knowledge of the fact that their customers *may* use that equipment to make unauthorised copies of copyrighted material. In the view of the Court, there was no precedent in the law of copyright for the imposition of vicarious liability merely on the showing of such fact.

Notes of dissent were struck by Justice Blackmun, who wrote an opinion on behalf of himself and three other judges. The learned judge noted that there was no private use exemption in favour of making of copies of a copyrighted work and hence, unauthorised time-shifting would amount to copyright infringement. He also concluded that there was no fair use in such activity that could exempt it from the purview of infringement. The dissent held the manufacturer liable as a contributory infringer and reasoned that the test for contributory infringement would only be whether the contributory infringer had *reason to know or believe* that infringement would take place, and *not whether he actually knew of the same*. Off-the-air recording was not only a foreseeable use for the Betamax, but also its intended use, for which Sony would be liable for copyright infringement.

[3] Sony Corp. v. Universal City Studios, Inc. (*Betamax*), 464 U.S. 417 (1984).

This dissent has considerably influenced the seemingly contrarian position taken by the majority in the subsequent decision, *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*[4] This case called into question the liability of websites that facilitated peer-to-peer (P2P) file-sharing. Re-formulating the test for copyright infringement, the U.S. Supreme Court held that "*one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties*." In re-drawing the boundaries of contributory infringement, the Court observed that contributory infringement is committed by any person who intentionally induces or encourages direct infringement, and vicarious infringement is committed by those who profit from direct infringement while declining to exercise their right to limit or stop it. When an article of commerce was good for nothing else but infringement, there was no legitimate public interest in its unlicensed availability and there would be no injustice in presuming or imputing intent to infringe in such cases. This doctrine would at the same time absolve the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and would limit the liability to instances of more acute fault than the mere understanding that some of the products shall be misused, thus ensuring that innovation and commerce are not unreasonably hindered.

The Court distinguished the case at hand from the *Betamax* case, and noted that there was evidence here of active steps taken by the respondents to encourage direct copyright infringement, such as advertising an infringing use or instructing how to engage in an infringing use. This evidence revealed an affirmative intent that the product be used to infringe, and an encouragement of infringement. Without reversing the decision in *Betamax*, but holding that it was misinterpreted by the lower court, the Court observed that *Betamax* was not an authority for the proposition that whenever a product was capable of substantial lawful use, the producer could never be held liable as a contributor for the use of such product for infringing activity by third parties. In the view of the Court, *Betamax* did not displace other theories of secondary liability. This other theory of secondary liability applicable to the case at hand was held to be the inducement rule, as per which any person who distributed a device with the object of promoting its use to infringe copyright, as evidenced by clear expression or other affirmative steps taken to foster infringement, would be liable for the resulting acts of infringement by third parties. However, the Court clarified that *mere knowledge of infringing potential or of actual infringing uses would not be enough* under this rule to subject a distributor to liability. Similarly, ordinary acts incident to product distribution, such as offering

[4] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. (*Grokster*), 545 U.S. 913 (2005).

customers technical support or product updates, support liability, etc. would not by themselves attract the operation of this rule. The inducement rule, instead, premised liability on *purposeful, culpable expression and conduct*, and thus did nothing to compromise *legitimate* commerce or discourage innovation having a *lawful* promise.

These seemingly divergent views on secondary infringement expressed by the U.S. Supreme Court are of significant relevance for India, due to the peculiar language used in the Indian Copyright Act, 1957 (hereinafter, "the Act"). As I will seek to show, this language has been retained even in the amendments of 2012, thus casting doubts on the efficacy of the fair use model that they legitimise. The starting point for this enquiry is Section 51 of the Act, which defines infringement. This provision bifurcates the two types of infringement, i.e., primary and secondary infringement, without indicating so in as many words. While Section 51(a)(i) speaks to primary infringement, 51(a)(ii) and 51(b) renders certain conduct to be secondary infringement. Even here, there is an important distinction between Sections 51(a)(ii) and 51(b). The former exempts the alleged infringer from liability if he can establish that *he was not aware and had no reasonable ground for believing that* the communication to the public, facilitated through the use of his "place", would amount to copyright infringement. The latter, on the other hand, permits no such exception. Thus, any person, who makes for sale or hire, or by way of trade, displays or offers for sale or hire, or distributes for the purpose of trade, or publicly exhibits by way of trade, or imports into India, any infringing copies of a work, shall be liable for infringement, without any specific *mens rea* required to attract such liability. It is in the context of the former provision, i.e., Section 51(a)(ii) that the liability of certain file-sharing websites for copyright infringement has arisen.

The *Myspace* Litigation and Secondary Infringement

In *Super Cassettes Industries Ltd. v. Myspace Inc.*,[5] the defendant was running a website that facilitated the sharing of media content by users/subscribers. The plaintiff, a leading sound recording and video label, alleged that the defendant, by providing a search and indexing function that allowed users to search for video/sound recordings and play such content on a computer, promoted copyright infringement. The plaintiff alleged both primary and secondary infringement on the part of the defendant. The plaintiff's case for primary infringement was that the defendant authorised the communication of the copyrighted works of the plaintiff to members of the public without

[5] Super Cassettes Industries Ltd. v. Myspace Inc. (*Myspace*), MIPR 2011 (2) 303.

the plaintiff's consent. To support the plea of secondary infringement, the plaintiff relied on Section 51(a)(ii) of the Act.

Rejecting the primary infringement plea raised by the plaintiff, the Delhi High Court held that although authorising an act which was part of the owner's exclusive right under Section 14 would no doubt amount to primary infringement under Section 51(a)(i), such authorisation required something more than merely providing the means to communicate the work to the public or providing the place for such communication. Explaining the level of involvement required for being a primary infringer on the ground of authorisation of infringement, the High Court held that active participation, inducement, or approval was a necessary ingredient to establish authorisation. The High Court clarified that knowledge of the fact that certain acts were infringing in character was different from active participation in, or any inducement of, such acts. The Court concluded that merely providing the means for infringement would not establish control, and therefore, any person providing such means could not be said to have approved or countenanced such act.

However, on the secondary infringement plea, the High Court, with all due respect, adopted a fairly dangerous yardstick to define the expression "*was not aware and had no reasonable ground for believing*" found in Section 51(a)(ii). The first error committed by the Court was in equating physical space and the virtual world, and assuming that the word "place" in this provision would automatically apply to the internet. To justify the view, the Court relied upon certain prior precedents on statutory interpretation to the effect that the language used in a statute must be given dynamic meaning to accommodate technological changes. These judgments were extremely fact-sensitive and most often involved situations where the regulation in question could realistically be extended to the new technology. The internet and physical space can perhaps be equated while drawing parallels between domain name infringement and passing off due to the common nature of the property involved, i.e., the identity of the person or business source identifier. However, the regulatory laws applicable to the control of physical property cannot be extended to the virtual world in similar fashion. Section 51(a)(ii) is, in effect, a provision that regulates control of physical property, by casting the onus upon the owner or possessor of the property to ensure that his place is not used for copyright infringement. The natural presumption is that this actor is indeed in a position to control the use to which his property can be put. This presumption does not hold good at all in the case of the internet. The architecture of the internet is such that an individual has much less control over what can be termed as his "space", whether it be an e-mail account, a page in a social networking website, or a website "managed" by him. Hence, it was erroneous in the first

place, to have applied a provision such as Section 51(a)(ii), worded with the specific purpose of fixing liability on a person having control over a physical space, to a similar actor in the online world, because the level of control in the hands of the latter is much lesser.

The second error was in interpreting the safe harbour provision contained in this section in a manner highly inconsistent with the spirit of other internet regulations, such as the Information Technology Act, 2000 (hereinafter, "the IT Act"). This again stemmed from the previous error, i.e., assuming that a person has *reasonable ground of belief* in respect of activities that go on in his backyard, except in certain limited situations. This assumption is valid in the case of physical spaces, and the actor who owns or possesses the same would indeed be in the best position to ascertain what really goes on. In the virtual world, this assumption breaks down and it is self-evident to any internet user that the level of control over any information that passes through our Twitter handles, Facebook status updates and so on, is quite low. Axiomatically, the situations for which we are exempt from liability for failing to regulate should be much higher in the latter scenario. The Delhi High Court completely ignored this perspective. While furnishing cause for its conclusion that the defendant was in a position of such reasonable belief as to the infringing activity, the Court relied on facts such as the revenue model of the defendant, which depended largely on advertisements displayed on the web pages, and automatically generated advertisements that would come up for a few seconds before the infringing video clips started playing. Shockingly, the Court even considered relevant the fact that the defendant provided safeguards such as hash block filters, take-down-stay-down functionality and rights management tools operational through fingerprinting technology, to prevent or curb infringing activities on its website. This, in the view of the Court, made it evident that the defendant had a *reasonable apprehension or belief* that the activities on the website *could* infringe someone else's copyright, including that of the plaintiff.

Once the Court had committed an error of such alarming proportions, having misunderstood the internet's architecture and the role and responsibilities of various actors therein, it was but natural for its interpretation of the safe harbour provisions in the Information Technology Act, 2000 to be coloured by such error. The defendant had, as an argument of last resort, contended that it was

an intermediary under Section 2(w)[6] of the IT Act, and thus stood protected under Section 79[7] of the same. Rejecting this contention, the Court reasoned that while the fulfilment of either one of the conditions under Section 79(2)(a) or 79(2)(b) would suffice, the immunity under Section 79(1) would not be available unless the due diligence requirement under Section 79(2)(c) was mandatorily satisfied along with the condition in Section 79(2)(a) *or* 79(2)(b). Coming to each sub-clause, the Court held that Section 79(2)(a) was not attracted as the function of the defendant was not confined to *only* providing access to the communication system where the third party information was stored, transmitted or hosted. Section 79(2)(b), to be attracted, required all three conditions mentioned therein to be satisfied. Since the defendant was already found to be modifying the content uploaded on its website, the Court held that the condition of non-modification of the

---

[6] "[I]ntermediary", with respect to any particular electronic records [sic], means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

Information Technology Act (2000), § 2(w).

[7] Exemption from liability of intermediary in certain cases – (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if–

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not –

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if –

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation – For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

Information Technology Act (2000), § 79.

information contained in the transmission was unfulfilled. Section 79(2)(c) was also held to be inapplicable, as the Court explained that such due diligence was required while the intermediary was discharging its duties. Thus, if the defendant was put to notice about the rights of the plaintiff in certain works, the defendant had to conduct a preliminary check in all the cinematographic works relating to Indian titles before communicating the works to the public, rather than falling back on post-infringement measures. The defendant's act of permitting the user to upload content on its server, and then modifying the same, was held to be contrary to the due diligence requirement. In the view of the Court, this conduct signified that the defendant had the chance to keep a check on the works, which the defendant avoided making use of for reasons best known to it. With all due respect, this view is erroneous as the modification of content was only auto-generated and done as part of the business model of the service provider, and happened regardless of the infringing or non-infringing character of the content uploaded onto its server. The view taken by the Court could potentially cripple a novel business model by rendering the service provider a pirate in the eyes of the law.

Website Blocking Orders and Intermediary Liability

The development in the *Myspace* case has to be considered along with the issuance of widely worded orders blocking access to websites, which courts in India have been granting of late.[8] The strategy employed by counsel representing the copyright owner in such cases is to seek injunctive relief against various John Does, i.e., unknown infringers, as well as to implead different internet service providers ('ISPs') as defendants along with such John Does. The permissibility of this strategy was called into question before the Madras High Court in *R.K. Productions Pvt. Ltd. v. B.S.N.L.*[9]

This case arose out of John Doe orders, or their Indian variant, Ashok Kumar orders, sought in respect of the Tamil film "3", which enjoyed considerable pre-release buzz due to its song "Kolaveri Di". The producers of the film wanted an omnibus order against all websites that hosted torrents or links facilitating access to or download of the film, apprehending that such electronic access would be made available immediately after the film's release due to the pre-release

[8] Reliance Big Entertainment Pvt. Ltd. v. Multivision Network, C.S. (O.S.) No. 3207/2011, I.A. No. 20510/2011 (Delhi High Court Dec. 19, 2011) (order), *available at* http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=269404&yr=2011; Sagarika Music Pvt. Ltd. v. Dishnet Wireless Ltd., C.S. No. 23/2012, G.A. No. 187/2012 (Calcutta High Court Jan. 27, 2012) (order), *available at* http://www.indiankanoon.org/doc/147345981/.

[9] R.K. Productions Pvt. Ltd. v. B.S.N.L. (*R.K. Productions*), (2012) 5 LW 626.

popularity. The Madras High Court initially granted an *ex parte* order.[10] A plain reading of this order made it clear that the known defendants, i.e., the ISPs, and the unknown Ashok Kumars, were restrained only from infringing the copyright in the specific cinematographic film/motion picture "3" through different means. However, the operationalisation of this order for a period of around two months after it was pronounced resulted in the blocking of access to various torrent and file-sharing websites.[11] The other problem with this order was the possibility of hauling up ISPs for contempt, upon failure to effectively implement this order. This prompted the ISPs to file applications under Order VII, Rule 11 of the Civil Procedure Code, 1908, seeking rejection of the plaint on the ground that the suit against them was barred by law.

In the *R.K. Productions* case, the Madras High Court has dismissed these applications for rejection of the plaint, after accepting the contention that the ISPs are necessary parties to the suit as the act of piracy occurs through the channel or network provided by them. The High Court has in fact relied on the decision in the *Myspace* case as well as given independent reasoning to conclude that the ISPs are liable for infringement. This is evident from the view taken by the Court on the safe harbour provision in Section 79 of the IT Act. Relying on the proviso to Section 81, the Court held that the exemption from intermediary liability carved out in Section 79 would not apply to cases of copyright infringement under Section 51(a)(ii) of the Copyright Act, 1957. This is totally incorrect as the proviso to Section 81 only mandates that "nothing contained in this Act shall restrict any person *from exercising any right conferred under* the Copyright Act". This then would bring us back to the language contained in Section 51(a)(ii), wherein the copyright owner would enjoy the *right to maintain an action of infringement* only if the alleged infringer was either aware or had reasonable ground to believe that the communication to the public was infringing in character. By holding that the proviso to Section 81 would override the exemption from liability in Section 79, the Madras High Court is in effect saying that an ISP, whose activity is restricted to facilitating the

---

[10] *R.K. Productions*, C.S. No. 208/2012, O.A. No. 230/2012 (Madras High Court Mar. 29, 2012) (order), *available at* https://docs.google.com/file/d/0Bxi2TzVXul5ZUl9EclRQZXlRdVdUb3c2S3EwSk1Udw/edit?pli=1.

[11] This prompted the Court to clarify the interim injunctions *vide* its common order dated June 22, 2012, in the following manner:

> The order of interim injunction, dated 29.3.2012 and 25.4.2012 passed in O.A.No.230 of 2012 in C.S.No.208 of 2012 and O.A.No.358 of 2012 in C.S.No.294 of 2012 respectively are hereby clarified that the interim injunction is granted only in respect of a particular URL where the infringing movie is kept and not in respect of the entire website. Further, the applicant is directed to inform the respondents/ defendants about the particulars of URL where the infringing movie is kept and on such receipt of particulars of URL from the plaintiff/applicant, the defendants shall take necessary steps to block such URLs within 48 hours.

technical transmission of information, can be imputed with reasonable grounds of belief that various communications that happen through the use of its network amount to copyright infringement. This is indeed shocking, and goes way beyond the decision in the *Myspace* case as well.

The other infirmity with this order is that it is *per incuriam*. The counsel appearing for both sides, i.e., the content owner and the ISPs, do not seem to have brought the factum of notification of the Copyright (Amendment) Act, 2012 about a month prior to the actual date of hearing in this case, to the Court's attention. A bare perusal of the newly introduced Sections 52(1)(b) and 52(1)(c), reproduced above, alone makes it abundantly clear that their content posed significant relevance to the issue at hand in the *R.K. Productions* case. Unfortunately, the Court missed out on the opportunity to be the first in the country to take a hard look at the correct interpretation of Sections 52(1)(b) and 52(1)(c), a task left now for us to undertake in the coming years. The author hence avails this opportunity to develop some of the interpretive possibilities.

Interpreting Section 52(1)(b) – The "Mere Conduit" Exception in U.K.

A plain reading of Section 52(1)(b) of the Copyright Act makes it clear that an entity, which carries on the sole activity of facilitating the technical process of electronic transmission or communication of infringing works to the public, or is in other words a "mere conduit", can in no situation be held liable for copyright infringement. There is no room for fixing any kind of liability on such entities, including contributory or vicarious liability. As a necessary corollary, the decision in the *R.K. Productions* case is incorrect as no suit for infringement would be maintainable against ISPs, who are solely facilitating such electronic transmission in a technical manner. However, it is still debatable whether ISPs can be impleaded as parties to a copyright infringement action on the basis that the current legal regime casts a duty on ISPs to remove, or disable access to, infringing content once they are put to notice of such infringement. This dichotomy between liability for infringement on the one hand and a general duty to assist in the prevention of infringement on the other is explained clearly by the Chancery Division in *Twentieth Century Fox Film Corporation v. British Telecommunications Plc.*[12]

[12] Twentieth Century Fox Film Corp. v. British Telecommunications Plc. (*Newzbin2*), [2011] EWHC 1981 (Ch).

In the *Newzbin2* case, the Chancery Division took note of the safe harbour provisions created by the E-Commerce Directive,[13] particularly Articles 12, 13 and 14 that deal with acting as a "mere conduit", caching and hosting respectively. The interesting feature with the "mere conduit" exception, which in all other respects is akin to the exception contained in Section 52(1)(b) of the Copyright Act, 1957, is the additional presence of Article 12(3). This provision clarifies that the "mere conduit" exception shall not stand in the way of a court or administrative authority requiring the service provider to terminate or *prevent* an infringement. Article 18 of this Directive also casts an obligation upon Member States to ensure that court actions available under national law permit the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved. Similarly, the Court looked into the Information Society Directive,[14]Article 8(3) of which provides that "Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right." This Directive was transposed into the domestic law of U.K. by the Copyright and Related Rights Regulations 2003, SI 2003/2498, resulting in the insertion of Section 97A in the Copyright, Designs and Patents Act, 1988. This provision empowers the Court to grant an injunction against a service provider who has actual knowledge of another person using his service to infringe copyright, such as where the service provider is given sufficient notice of the infringement. Finally, the Chancery Division also took note of the Enforcement Directive,[15] Article 11 of which provides that Member States shall ensure that copyright owners are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right. This entire legislative scheme compelled the Court in the *Newzbin2* case to conclude that an order of injunction could be granted against ISPs who are "mere conduits", restraining them from providing access to websites that indulged in mass copyright infringement. The Court reasoned that the language used in Section 97A did not require knowledge of any particular infringement but only a more general kind of knowledge about certain persons using the ISPs' services to infringe copyright. Thus, it is seen that in the United Kingdom, though a "mere conduit" activity is not considered

---

[13] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market. This Directive was transposed into the domestic law of UK by the Electronic Commerce (EC Directive) Regulations 2002, SI 2002/2013.

[14] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society.

[15] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, 2004 O.J. (L 157). This Directive was transposed into the UK domestic law primarily by the Intellectual Property (Enforcement, etc.) Regulations 2006, SI 2006/1028.

infringement, the concerned ISP can be directed by the Court to block access to a website that hosts infringing content on the basis of the above legislative scheme. The enquiry should therefore be directed towards whether India has a similar scheme for copyright enforcement.

The IT Act – An Inapplicable Scheme for Website Blocking

The IT Act, read with the recently framed Information Technology (Intermediary Guidelines), 2011 which came into effect on April 4, 2011, provides for a duty that could be thrust upon even "mere conduit" ISPs to disable access to copyrighted works. This is due to the presence of Section 79(2)(c) of the Act, which makes it clear that an intermediary shall be exempt from liability only where the intermediary observes due diligence and complies with other guidelines framed by the Central Government in this behalf. Moreover, Section 79(3) provides that the intermediary shall not be entitled to the benefit of the exemption in Section 79(1) in a situation where the intermediary, upon receiving actual knowledge that any information, data, or communication link residing in or connected to a computer resource controlled by the intermediary, is being used to commit an unlawful act, fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner. Rule 4, when read along with Rule 2(d) of these Guidelines, casts an obligation on an intermediary on whose computer system copyright infringing content has been *stored, hosted or published*, to *disable* such information within thirty six hours of it being brought to its actual knowledge by any affected person.

One way of understanding and harmoniously interpreting the provisions of the IT Act and the Guidelines therein along with the recent amendments to the Copyright Act, is to contend that the issue of copyright infringement by "mere conduit" ISPs is governed by Section 52(1)(b), which completely absolves them of any liability, while that of enforcement of copyright through the medium of such ISPs is governed by the IT Act. This bifurcation suffers from the difficulty that Section 79 of the IT Act is not an enforcement provision. It is a provision meant to exempt intermediaries from certain kinds of liability, in the same way as Section 52 of the Copyright Act. This provision, read with Section 81, makes it clear that the IT Act does not speak to liability for copyright infringement. From this, it has to necessarily follow that all issues pertaining to liability for such infringement have to be decided by the provisions of the Copyright Act. Therefore, the scheme in the IT Act read with the Intermediaries Guidelines cannot confer additional liability for copyright infringement on ISPs, where the Copyright Act exempts them from liability. More to the point, the intermediary cannot be liable for copyright infringement in the event of non-compliance with Section 79(3) or Rule 4 of the Intermediaries Guidelines read with Section

79(1)(c) of the IT Act. Rule 4 of the Intermediaries Guidelines, 2011 to the extent that it renders intermediaries outside the protective ambit of Section 79(1), upon failure to disable access to copyrighted content, is of no relevance as "mere conduits" have already been exempted from liability under Section 52(1)(b). Moreover, since these provisions in the IT Act do not deal with enforcement measures such as injunction orders from the Court to disable access to infringing content in particular or infringing websites in general, it would be wrong to contend that the scheme in India is similar to the one in the United Kingdom, where the issue of infringement has been divorced from that of enforcement.

To conclude, Section 52(1)(b) is a blanket "mere conduit" exemption from liability for copyright infringement that stands uninfluenced by the presence of Section 79 of the IT Act or the Intermediaries Guidelines. In the absence of a legislative scheme for enforcement in India akin to Section 97A of the U.K. Copyright, Designs and Patents Act, 1988, Indian Courts cannot grant an injunction directing such "mere conduit" ISPs to block access to websites in general or infringing content in particular, and any such action is not even maintainable in law post the insertion of Section 52(1)(b). The decision to the contrary in the *R.K. Productions* case is incorrect.

Interpreting Section 52(1)(c) – *Myspace* and Interpretive Concerns

The liability for copyright infringement of file-sharing websites and other service providers who perform roles beyond that of a "mere conduit" shall again be governed solely by the Copyright Act and not the IT Act, for the same reasons advanced above in the context of Section 52(1)(b). However, in the case of such file-sharing networks, the important issue is whether a safe harbour has really been created. One striking distinction between clauses (b) and (c) is the presence of the phrase "*unless the person responsible is aware or has reasonable grounds for believing*" in the latter provision. As a result, if a file-sharer has such reasonable grounds of belief, the exemption from liability would not be attracted.

The actual concern for file-sharing websites is the similarity in language employed in Sections 51(a)(ii) and 52(1)(b) of the Copyright Act. As already seen above, the *Myspace* case interprets this expression in a wide manner, to include even conduct such as the inclusion of system generated advertisements, the introduction of specific measures to curb the possibility of infringing content being made available, and the receipt of a general list from the content owner that contains the names of all their copyrighted works without identifying specific acts of infringement in respect of these works. It is reiterated that this standard is incorrect as it confuses the possibility of

regulation over physical space with that over the internet, paying no heed to specificities of the latter medium and its architecture.

Assuming that the interpretation in the *Myspace* case will be discarded while giving meaning to the fair use exception in Section 52(1)(c), this provision is again attracted only where the storage of the infringing file is transient or incidental to the act of providing links or access to the work. A possible rationale for the usage of the expression "transient or incidental" could be to distinguish legitimate file-sharing websites that operate in content neutral fashion from those where the file-sharing website actively promotes the perpetration of piracy and the storage of the file is no longer incidental. In the latter kind of situation, the file-sharing website would also be liable under the doctrine of contributory liability for communication of the copyrighted work to the public, using the standard laid down in *Grokster*.

Finally, Section 52(1)(c), as opposed to Section 52(1)(b), is not a blanket exemption and permits the issuance of notice to the file-sharing website to remove infringing content. This is indeed a healthy practice and can result in a culture of self-regulation, which in the author's view, is the only effective kind of regulation when it comes to the internet.

IP ADDRESSES AND EXPEDITIOUS DISCLOSURE OF IDENTITY IN INDIA

Prashant Iyengar[*]

Concomitant with the proliferation of cybercrime in India has been the use of Internet Protocol (IP) addresses by law enforcement agencies to track down criminals. While useful in many situations, the potential for misuse of this information raises important concerns for the privacy of individuals online. This note reviews the statutory mechanisms regulating the retention and disclosure of IP addresses by internet companies in India. It identifies and analyses the four broad sources to which the regime of IP Address disclosure by Internet Service Providers (ISP) may be traced: under the (i) operating licenses issued under the Telegrah Act, 1885, (ii) Information Technology Act, 2000, (iii) Code of Criminal Procedure, 1973 (hereinafter, "the Cr.P.C.") and (iv) contractual agreements between users and ISPs. It concludes that the various layers of Indian law create an atmosphere that is intensely hostile to the withholding of such information by ISPs and intermediaries. Despite this, the author submits that there remains scope for optimism.

Introduction

With the rise in the number of users in the past decade, the internet has become an extremely fraught space that has been frequently used for the perpetration of a range of cyber crimes, including extortion, defamation and financial fraud. In a revealing statistic, in 2010, the Mumbai Police reportedly "received 771 complaints about internet-related offences, *319 of which were from women who were the victims of fake profiles, online upload of private photographs and obscene emails*."[1] This high incidence of women victims indicates that the relatively anonymous 'open' architecture of the internet has yielded disempoweringly discriminatory consequences for women, who tend to be easy targets of humiliation, harassment or blackmail online.

---

[*] Prashant Iyengar is Assistant Professor & Assistant Director, Centre for Intellectual Property Rights Studies. He has an (LL.M.) with honors from Columbia Law School and a B.A.B.L. (Hons.) from NALSAR, University of Law, Hyderabad. Earlier, he was Lead Researcher with Privacy India, Bangalore; Legal Aid Manager with Rural Development Institute, Hyderabad; Researcher & Lawyer with Alternative Law Forum, Bangalore and was Guest faculty with Christ Law College, Bangalore.

[1] Mateen Hafeez, *A tangled web of vengeance*, TIMES OF INDIA (Mar. 28, 2011, 5:44 AM), http://articles.timesofindia.indiatimes.com/2011-03-28/mumbai/29353669_1_boyfriend-social-networking-police-officer.

Law enforcement authorities in India have not exactly lagged behind in bringing these new age cyber criminals to book, and have set up special 'Cyber Crime Cells' in different cities to combat crimes on the internet. These cells have been particularly adept at using IP addresses' information to trace the individuals responsible for these crimes. Very briefly, an Internet Protocol address (hereinafter, "IP address") is a numeric label – a set of four numbers (e.g., 202.54.30.1) – that is assigned to every device (e.g., computer, printer, mobile phone) participating on the internet.[2] Website operators (such as Google) and Internet Service Providers ("ISPs", such as Airtel or BSNL) typically maintain data logs that track the online activity of every IP address that accesses their services. Although IP addresses refer to particular computers – not necessarily individual users – it is possible, through further investigation, to trace these addresses backwards to expose the individual behind the computer.[3] As even a casual Google search with the phrase "IP, police, India" would reveal, police authorities in different cities in India have successfully and quite happily employed this new technology to trace culprits.

However, along with its utility in the detection of crime, the tracking of persons by their IP addresses is potentially invasive of individuals' privacy – itself a weak, embattled legal right in India. In the absence of a culture of strict adherence to the 'rule of law' by the police apparatus in India, the unbridled ability to track persons through IP addresses has the potential of becoming an extremely oppressive tool of pervasive surveillance.

In addition, several alarming incidents in the past year have made it clear that the Indian Government has found in this technology a reliable ally with which it may stamp out political dissent, or even satire and unfavourable comment, on the internet. These incidents raise questions of free speech and censorship, which are superadded to the concerns of privacy.

In this short note, I review the statutory mechanism regulating the retention and disclosure of IP addresses by internet companies in India. Increasingly in Indian scholarship and in the courts, it has become uncommon to attempt to tie executive action to any specific legislative mandate. In order to

---

[2] *IP address*, WIKIPEDIA, http://en.wikipedia.org/wiki/IP_Address (last visited June 15, 2011).

[3] McIntyre, Joshua J., Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information (August 15, 2010). DePaul Law Review, Vol. 60, No. 3, 2011. Available at SSRN: http://ssrn.com/abstract=1621102 [Accessed June 21, 2012]

provide context, I begin with a compilation of anecdotes on how various law enforcement authorities in India have used IP address information to trace individuals responsible for particular crimes.

Examples of Use and Abuse by Indian Authorities

As mentioned above, over the past several years, internet media has been humming with stories which indicate the extent to which IP addresses have become a useful and frequently deployed weapon in the arsenal of law enforcement agencies and courts:

a) In May 2010, an Army officer stationed in Mumbai was arrested for distributing child pornography from his computer.[4] He was traced by the Mumbai Police after the German Federal Police alerted Interpol that objectionable pictures were being uploaded from the IP address he was using.

b) In February 2011, Cyber Crime Police in Mumbai sought the IP address details of a user who had posted 'Anti Ambedkarite' content on Facebook, the popular social networking website.[5]

c) In February 2008, the internet search company Google was ordered by the Bombay High Court to reveal "particulars, names and the address of the person" who had posted defamatory content against a company on Google's blogging service, Blogger.[6]

---

[4] *Army officer held in city for child porn*, TIMES OF INDIA (May 8, 2010, 1:59 AM), http://articles.timesofindia.indiatimes.com/2010-05-08/mumbai/28292650_1_hard-disks-obscene-clippings-downloading.

[5] *Anti-Ambedkar page on Facebook blocked*, HINDUSTAN TIMES (Feb. 17, 2011, 2:45 AM), http://www.hindustantimes.com/Anti-Ambedkar-page-on-Facebook-blocked/Article1-663383.aspx.

[6] David Sarokin, *Google Ordered to Reveal Blogger Identity in Defamation Suit in India: Gremach Infrastructure vs Google India*, SAROKI6965 BLOG (Aug. 15, 2008), http://saroki6965.wordpress.com/article/google-ordered-to-reveal-blogger-l9cm7v116zcn-7/.

d) In September 2009, a man was arrested by the Delhi Police in Mumbai for blackmailing classical musician Anoushka Shankar. The culprit had allegedly hacked into her e-mail account and downloaded copies of personal photographs. He was traced by using his IP address.[7]

e) In April 2010, the Gurgaon Police arrested a teenage boy for allegedly posting obscene messages about an actress on Facebook. The newspaper account reports that:

> During investigations, the police browsed through several service providers and finally zeroed in on BSNL, which helped them trace the sender's IP address to someone called 'Manoj Gupta' in Gurgaon. A team of policemen were sent to Gurgaon but the personnel found out that Manoj Gupta was [a] fictitious name which the teenager was using in his IP address. The police arrested the accused as well as seized the hardisk [sic] of his personal computer.[8]

f) In February 2011, the police traced a missing boy who had run away from home, by following the IP address trail he left when he updated his Facebook profile status.[9]

g) In March 2013, the Mumbai Police tracked down a girl who had sent an e-mail to a newspaper threatening to commit suicide on account of her poor 12th standard examination results.[10]

What is clearly evident from these accounts is a growing awareness and enthusiasm on the part of Indian law enforcement agencies to use IP address trails as a routine part of their criminal investigation process. While this is not unwelcome, considering the kinds of grievances listed above and the backdrop of a dismal record of criminal enforcement in India, there is also a flip side to consider. In

---

[7] *Delhi police arrest man for blackmailing Anoushka Shankar*, REDIFF (Sept. 20, 2009, 4:51 PM), http://news.rediff.com/report/2009/sep/20/police-arrest-man-for-blackmailing-anoushka-shankar.htm.

[8] S. Ahmed Ali, *Cyber cell nets Delhi teen for lewd online posts*, TIMES OF INDIA (Apr. 29, 2010, 6:11 AM), http://articles.timesofindia.indiatimes.com/2010-04-29/mumbai/28116011_1_cyber-cell-cyber-police-abusive-messages.

[9] Mateen Hafeez, *Police find runaway student "online"*, TIMES OF INDIA (Feb. 17, 2011, 1:42 AM), http://articles.timesofindia.indiatimes.com/2011-02-17/mumbai/28554314_1_social-networking-networking-site-sim-card.

[10] *Cop pep talk a balm for suicidal Class 12 girl*, DNA INDIA (Mar. 8, 2013, 6:45 AM), http://www.dnaindia.com/mumbai/1808695/report-cop-pep-talk-a-balm-for-suicidal-class-12-girl.

a shocking incident in August 2007, Lakshmana Kailash, a software engineer from Bangalore, was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut.[11] The police identified him based on IP address details obtained from Google and Airtel, Lakshmana's ISP. He was brought to Pune and jailed for fifty days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not clearly specified whether the suspect had posted the content at 1:15 p.m. or a.m.

Taking cognisance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered Airtel to pay Rs 2 lakh to Lakshmana as damages.[12] This incident sounds a cautionary note, amidst so many celebratory accounts, signalling that grave human rights abuses could result from the unbridled use of this technology.

In an eerily similar incident, in April 2011, a 65 year old man was arrested in Pune and later prosecuted for allegedly posting obscene photographs of a woman on Facebook. During the trial, it was realised that the police had arrested the wrong person since "the social media firm sent dates in the normal US format of 'month-day-year' (MM/DD/YY). But the police read it in the Indian format of 'day-month-year' (DD/MM/YY)." The newspaper account goes on to report that he has filed a Public Interest Litigation before the Supreme Court, seeking the framing of appropriate guidelines to ensure such errors do not recur. [13]

These are just a few out of scores of instances of Indian investigative authorities tracing culprits using IP addresses. The offences alleged range from blackmail to impersonation, and from defamation to planning terror attacks. Seldom in these cases has a court order actually been required by the agency that discloses the IP address of the individual.[14] Clearly, there seems to be a very easy relation between

---

[11] Anand Holla, *Wronged, techie gets justice 2 yrs after being jailed*, MUMBAI MIRROR (June 25, 2009, 3:14 AM), http://www.mumbaimirror.com/mumbai/others/Wronged-techie-gets-justice-2-yrs-after-being-jailed/articleshow/15934351.cms.

[12] *Id.*

[13] Utkarsh Anand, *Cops mix up dates, 65-yr-old in cyber soup*, INDIAN EXPRESS (Mar. 2, 2013, 2:39 AM), http://www.indianexpress.com/news/cops-mix-up-dates-65yrold-in-cyber-soup/1082000/0.

[14] This is not atypical. In the US, for instance, as Joshua McIntyre writes:

law enforcement agencies in India on the one hand, and Internet Service Providers and online services such as Google and Facebook on the other.

Google's own 'Transparency Report'[15] which provides statistics on the number of instances where Government agencies have approached the company demanding information or take-down, states that it received close to 4700 'data requests' from Indian authorities between January to December 2012 – ranking India 2nd globally in terms of such requests, behind the United States. That a high percentage – 64-66% – of these requests have reportedly been complied with indicates that within a short span of time, Indian authorities have discovered in Google a reliable and pliable ally in seeking information about their subjects. In 2007, Orkut, a social-networking website owned by Google, even entered into a co-operation agreement with the Mumbai Police in terms of which "'forums' and 'communities'" which contained "defamatory or inflammatory content" would be blocked, and the IP addresses from which such content had been generated would be disclosed to the police.[16]

> While various federal statutes protect similar data such as telephone numbers and mailing addresses as Personally Identifiable Information (PII), federal privacy law does not generally regard IP addresses as information worthy of protection. It has, therefore, become commonplace for litigants to subpoena ISPs to unmask online speakers. *Many ISPs have no reason to fight these subpoenas and readily give up their subscribers' names, addresses, telephone numbers, and other identifying data without demanding any court oversight or providing any notice to the subscriber. Even when courts become involved, a full consideration of the online speaker's privacy interests is far from certain*. (emphasis added)

MCINTYRE, *supra* note 3, at 5.

15 *Google Transparency Report: User Data Requests – India*, GOOGLE.COM, http://www.google.com/transparencyreport/userdatarequests/IN/ (last visited Apr. 4, 2013).

16 *Orkut's tell-all pact with cops*, ECONOMIC TIMES (May 1, 2007, 9:00 AM), http://articles.economictimes.indiatimes.com/2007-05-01/news/28459689_1_orkut-ip-addresses-google-spokesperson.

Although similar transparency reports are not forthcoming from the other Internet giants such as Hotmail,[17] Yahoo[18] or Facebook,[19] there is overwhelming anecdotal evidence that this co-operation has not been withheld by them.

In the sections that follow, I shall outline the legal framework that facilitates this co-operation between law enforcement authorities and web service providers.

Lawful Disclosure of IP Addresses

In this section, we are seeking a legal source for the compulsion of ISPs and intermediaries (including websites) to disclose IP address data. Are there any guidelines in Indian law on how much information must be disclosed, under what circumstances and for how long?

Broadly, there are four sources to which we may trace this regime of disclosure and co-operation. *First*, ISPs are required, under the operating license they are issued under the Telegraph Act, 1885, to provide assistance to law enforcement authorities which, under certain circumstances, include turning over all user records. *Secondly*, the Information Technology Act, 2000 (hereinafter, "the IT Act") contains provisions which empower law enforcement authorities to compel the disclosure of information from those in charge of any 'computer resources'. Reciprocally, 'intermediaries' – including ISPs and websites – are charged under new Rules under the IT Act with co-operating with government agencies on pain of exposure to financial liability. *Thirdly*, the Code of Criminal Procedure, 1973 (hereinafter, "the Cr.P.C.") defines the scope of police powers of investigation, which include powers to interrogate and summon information. *Fourthly*, individual subscribers enter into contracts with ISPs and web services which do not offer any stiff assurances of privacy with regard to IP address details.

---

[17] In June 2011, Hotmail supplied IP address details which enabled the Delhi Police to trace, with further assistance from Airtel, the sender of obscene e-mails to a noted actress. Mohit Sharma, *Priyanka Chopra's cousin harassed in Delhi*, MID-DAY (June 10, 2011), http://www.mid-day.com/news/2011/jun/100611-news-delhi-priyanka-chopra-cousin-Meera-Chopra-harrassed.htm.

[18] Alok K.N. Mishra, *Man who sent hoax email to DGP nabbed*, TIMES OF INDIA (Jan. 1, 2013, 4:50 AM), http://articles.timesofindia.indiatimes.com/2013-01-01/ranchi/36093637_1_hoax-email-cyber-cafe-hoax-mail.

[19] ANAND, *supra* note 14.

The sections that follow offer greater detail on each of these areas of the law.

1. Monitoring of Internet Users under the ISP Licenses

ISPs are regulated and operate under a license issued under the Telegraph Act, 1885. Section 5 of the Telegraph Act empowers the Government to take possession of 'licensed telegraphs' and to order interception of messages in cases of 'public emergency' or 'in the interest of the public safety'. Interception may only be carried out pursuant to a written order by an officer specifically empowered for this purpose by the State or Central Government. The officer must be satisfied that "it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence."20

Although the statute governs the actions of ISPs in general, more detailed guidelines regulating their behaviour are contained in the terms of the licenses issued to them, which set out the conditions under which they are permitted to conduct business. The Internet Services License Agreement, which authorises ISPs to function in India, contains provisions requiring telecom operators to safeguard the privacy of their consumers and to co-operate with government agencies when required to do so. Some of the important clauses in this Agreement are:

a) Part VI of the License Agreement gives the Government the right to inspect or monitor the ISPs' systems. The ISP is responsible for making facilities available for such interception.

b) Clause 32 under Part VI contains provisions mandating the confidentiality of information held by ISPs. These provisions hold ISPs responsible for the protection of privacy of

20 In 1997, in PUCL v. Union of India (AIR 1997 SC 568), the Supreme Court of India held that the interception of communications under this Section was unlawful unless carried out according to the procedure established by law. Since no Rules had been prescribed by the Government specifying the procedure to be followed, the Supreme Court framed guidelines to be followed before tapping of telephonic conversations. These guidelines have been substantially incorporated into the Indian Telegraph Rules in 2007. Rule 419A stipulates the authorities from whom permission must be obtained for tapping, the manner in which such permission is to be granted and the safeguards to be observed while tapping communication. The Rule stipulates that any order permitting tapping of communication would lapse (unless renewed) in two months. In no case would tapping be permissible beyond 180 days. The Rule further requires all records of tapping to be destroyed after a period of two months from the lapse of the period of interception.

communication, and to ensure that unauthorised interception of messages does not take place. Towards this, ISPs are required:

a. to take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and their business to which they provide service and from which they have acquired such information by virtue of that service, and shall use their best endeavours to secure that;

b. to ensure that no person acting on behalf of the ISPs divulges or uses any such information, except as may be necessary in the course of providing such service to the third party.

This safeguard, however, does not apply where:

i. the information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or

ii. the information is already open to the public and otherwise known.

c. to take necessary steps to ensure that any person(s) acting on their behalf observes confidentiality of customer information.

c) Clause 33.4 makes it the responsibility of the ISP to trace nuisance, obnoxious or malicious calls, messages or communications transported through its equipment.

d) Clause 34.8 requires ISPs to maintain a log of all users connected and the service they are using (mail, telnet, http etc.). The ISPs must also log every outward login or telnet through their computers. These logs, as well as copies of all the packets originating from the Customer Premises Equipment (CPE) of the ISP, must be available in real time to Telecom Authority. This clause forbids logins where the identity of the logged-in user is not known.

e) Clauses 34.12 and 34.13 require the ISP to make available a list of all subscribers to its services on a password protected website for easy access by Government authorities.

f) Clause 34.16 requires the ISP to activate services only after verifying the *bona fides* of the subscribers and collecting supporting documentation. There is no Regulation governing how long this information is to be retained.

g) Clause 34.22 makes it mandatory for the Licensee to make available "details of the subscribers using the service" to the Government or its representatives "at any prescribed instant".

h) Clause 34.23 mandates that the ISP maintain "all commercial records with regard to the communications exchanged on the network" for a period of "at least one year for scrutiny by the Licensor for security reasons and may be destroyed thereafter unless directed otherwise by the Licensor".

i) Clause 34.28(viii) forbids the ISP from transferring the following information to any person or place outside India:

    a. Any accounting information relating to subscribers (except for international roaming/billing) (Note: It does not restrict a statutorily required disclosure of a financial nature); and

    b. User information (except that pertaining to foreign subscribers using an Indian Operator's network while roaming).

j) Clause 34.28(ix) and (x) require the ISP to provide traceable identity of its subscribers and on request by the Government, must be able to provide the geographical location of any subscriber at any given time.

k) Clause 34.28(xix) stipulates that "in order to maintain the privacy of voice and data, *monitoring shall only be upon authorisation by the Union Home Secretary or Home Secretaries of the States/Union Territories.*" (It is unclear whether this is to operate as an overriding provision governing all the other clauses as well).

From the list above, it is very clear that by the terms of their licenses, ISPs are required to maintain extensive logs of user activity for unspecified periods. However, it is unclear, in practice, to what

extent these requirements are being followed by ISPs. For instance, an article in the Economic Times in December 2010 reports:

> The Intelligence Bureau wants internet service providers, or ISPs, to keep a record of all online activities of customers for a minimum of six months. *Currently, mobile phone companies and internet service providers do not keep online logs that track the web usage pattern of their customers. They selectively monitor online activities of only those customers as required by intelligence and security agencies, explained an executive with a telecom company.*[21] (emphasis added)

The same news report quotes Rajesh Chharia, President of the Internet Service Providers' Association of India, as saying, "[a]t present, we only keep a log of all our customers' Internet Protocol address, which is the digital address of a customer's internet connection."

The news report goes on to disclose the ambitious plans of the Intelligence Bureau to "put in place a system that can uniquely identify any person using the internet across the country" through "a technology platform where users will have to mandatorily submit some form of an online identification or password to access the internet every time they go online, irrespective of the service provider." Worryingly, the report goes on to discuss the setting up by the telecommunications department of:

> India's indigenously-built Centralised Monitoring System (CMS), which can track all communication traffic—wireless and fixed line, satellite, internet, e-mails and voice over internet protocol (VoIP) calls—and gather intelligence inputs. The centralised system, modelled on similar set-ups in several Western countries, aims to be a one-stop solution as against the current practice of running several decentralised monitoring agencies under various ministries, where each one has contrasting processing systems, technology platforms and clearance levels.

---

[21] Jogi Thomas Philip, *Intelligence Bureau wants ISPs to log all customer details*, ECONOMIC TIMES (Dec. 30, 2010, 11:50 AM), http://articles.economictimes.indiatimes.com/2010-12-30/news/27621627_1_online-privacy-internet-protocol-isps.

Although at the time of writing this CMS is not yet fully functional, its launch seems to be imminent and will inaugurate with it, an era of constant and continuous surveillance of all internet users.

2. Provisions under the Information Technology Act, 2000

The IT Act enables government agencies to obtain IP address details from intermediaries, including ISPs, by following a stipulated procedure. In addition, it enjoins intermediaries to co-operate with law enforcement agencies as a part of their due diligence behaviour.

In a parallel and seemingly conflicting move, the IT Act also requires intermediaries to observe stiff Data Protection norms. In the sub-sections that follow, we look at each of these provisions under the IT Act.

(1) Interception and Monitoring of Computer Resources

There are two regimes of interception and monitoring information, under separate sections of the IT Act. Both would seem capable of authorising government agencies access to IP addresses, among other information.

Section 69 deals with "[p]ower to issue directions for interception or monitoring or decryption of any information through any computer resource".[22]

In addition, the Government has been given a more generalised monitoring power under Section 69B, to "monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource."[23] This monitoring power may be used to aid a range of "purposes related to cyber security"[24]. "Traffic data" has been defined in the section to mean "any data identifying or purporting

[22] Information Technology Act (2000), § 69.

[23] Information Technology Act (2000), § 69B.

[24] The Monitoring Rules list 10 'cyber security' concerns for which monitoring may be ordered: (a) forecasting of imminent cyber incidents; (b) monitoring network application with traffic data or information on computer resource; (c) identification and determination of viruses/computer contaminants; (d) tracking cyber security breaches or cyber security incidents; (e) tracking computer resource breaching cyber security or spreading virus/computer contaminants; (f) identifying or tracking of any person who has contravened, or is suspected of having contravened, or being likely to contravene cyber security; (g) undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resource; (h) accessing stored information for enforcement of any provision of the laws relating to cyber security for the time being in force; and (i) any other matter relating to cyber security.

to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted."

Rules have been issued by the Central Government under both these sections[25] which are similar, although with important distinctions. These Rules stipulate the manner in which the powers conferred by the sections may be exercised.

The important difference between the two sections is that while Section 69 provides a mechanism whereby specific computer resources can be monitored in order to learn the contents of communications that pass through such resources, Section 69B by contrast provides a mechanism for obtaining 'meta-data' about all communications transacted using a computer resource over a period of time – their sources, destinations, routes, duration, time, etc., without actually learning the content of the messages involved. The latter type of monitoring is specifically in order to combat threats to 'cyber security', while the former can be invoked for a number of purposes such as the securing of public order and criminal investigation.[26]

However, this distinction is not very sharp – an interception order under Section 69 directed at a computer resource located in an ISP can yield traffic data in addition to the content of all communications. Thus, for instance, if a direction was passed ordering my ISP to intercept "all communications sent or received by Prashant Iyengar", the information obtained by such interception would include a resume of all e-mails exchanged, websites visited, files downloaded, etc. In such a case, a separate order under Section 69B would be unnecessary. An important clue about their relative importance may lie in the different purposes for which each section may be invoked, coupled with the fact that while directions under Section 69 can be issued by officers both at the central and state level, directions under Section 69B can only be issued by the Secretary of the Department of Information

---

[25] Respectively, the INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARDS FOR INTERCEPTION, MONITORING AND DECRYPTION OF INFORMATION) RULES (2009) and INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR MONITORING AND COLLECTING TRAFFIC DATA OR INFORMATION) RULES (2009).

[26] Section 69 lists the following grounds for which interception may be ordered: a) sovereignty or integrity of India; b) defense of India; c) security of the State; d) friendly relations with foreign States; e) public order; f) preventing incitement to the commission of any cognisable offence relating to above; or g) for investigation of any offence.

Technology under the Union Ministry of Communications and Information Technology.[27] This indicates that the collection of traffic data by the Government under Section 69B is intended to facilitate the securing of India's 'cyber security' from possible *external* threats – a defence function – while the interception powers under Section 69 are to be exercised for more domestic purposes as aids to police functions.

The Rules framed under Sections 69 and 69B contain important safeguards stipulating, *inter alia*, the following: a) who may issue directions; b) how the directions are to be executed; c) the duration they remain in operation; d) to whom data may be disclosed; e) confidentiality obligations of intermediaries; f) periodic oversight of interception directions by a Review Committee under the Telegraph Act; g) maintenance of records of interception by intermediaries; and h) mandatory destruction of information in appropriate cases.

Although these sections provide powerful tools of surveillance in the hands of the State, these powers may only be exercised by observing the rather tedious procedures laid down. In the absence of any data on interception orders, it is unclear as to what extent these powers are in fact being used in the manner laid down. Certainly, from the instances cited at the beginning of this paper, the police departments in the various states do not seem to need to invoke these powers in order to obtain IP address information from ISPs or websites; this information appears to be available to them merely for the asking. How do we account for this unquestioning pliancy on the part of the ISPs?

In February 2011, Reliance Communications, a large telecom service provider, disclosed to the Supreme Court that over a 150,000 telephones had been tapped by it between 2006 and 2010 – almost 30,000 a year. A majority of these interceptions were conducted based on orders issued from state police departments – whose legal authority to issue them is suspect. New Rules framed under the Telegraph Act in 2007 required such orders to be issued only by a high-ranking Secretary in the Department/Ministry of Home Affairs.[28] The willing compliance by Reliance with the police's

[27] Rule 2(d), INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR MONITORING AND COLLECTING TRAFFIC DATA OR INFORMATION) RULES (2009).

[28] Telegraph (Amendment) Rules (2007).

requests indicates both their own as well as the police's blithe unawareness about the change in the regime governing tapping. Things seem to have continued just as before through pure inertia.

To return to the question about why ISPs comply with police requests, it is conceivable that this same inertia, and an intuitive confidence both on the part of the police and the ISPs that they would not be made to answer for their disclosures, is what explains the ready and expeditious access that ISPs give police departments to IP address details.

In the next sub-section, we examine intermediary liability rules which require intermediaries to positively disclose personal information to law enforcement authorities.

(2) Data Protection Rules

Section 43A of the IT Act obliges corporate bodies who "possess, deal or handle" any "sensitive personal data" to implement and maintain "reasonable" security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.

In April 2011, the Central Government notified Rules[29] under section 43A of the Information Technology Act in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold. Since traffic data, including IP address data, is one kind of personal information that ISPs hold, and since all ISPs are "body corporates", these Rules apply to them equally and define the terms on which they may deal with such information.

Rule 3 of these Rules designates various types of information as 'sensitive personal information', including passwords, medical records, etc.[30] Significantly, for the purposes of this paper, IP address details are not included in this list.

---

[29] INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES (2011).

[30] The full list under Rule 3 includes: password; financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above as provided to body corporates for providing service; and any information received under the above by body corporates for processing, stored or processed under lawful contract or otherwise.

Body Corporates are forbidden from collecting any information without prior consent in writing for the proposed usage. Further, Rule 5 states that sensitive personal information may not be collected unless: (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and (b) the collection of the information is necessary for that purpose.

Rule 4 enjoins a body corporate or its representative who "collects, receives, possess [sic], stores, deals or handles" data to provide a privacy policy "for handling of or dealing in user information including sensitive personal information". This policy is to be made available for view by such "providers of information"[31] including on a website. The policy must provide the following details:

(i) Clear and easily accessible statements of its practices and policies;

(ii) Type of personal or sensitive information collected;

(iii) Purpose of collection and usage of such information;

(iv) Disclosure of such information as provided in Rule 6;[32]

(v) Reasonable security practices and procedures as provided under Rule 8.

Rule 6 enacts as a general rule that disclosure of information "by the body corporate to any third party shall require prior permission from the provider of such information". Consent is, however, not required "where disclosure is necessary for compliance of a legal obligation". This is further fortified by a proviso to the rule which stipulates the mandatory sharing of information "without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences." In such a case, the Government agency is required to "send a request in

[31] "Provider of data" is not the same as an individual to whom the data pertains, and could possibly include intermediaries who have custody over the data. I feel this privacy policy should be made available for view generally – and not only to providers of information. In addition, it might be advisable to mandate registration of privacy policies with designated data controllers.

[32] This is well framed since it does not permit body corporates to frame privacy policies that detract from Rule 6.

writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information." The government agency is also required to "state that the information thus obtained will not be published or shared with any other person."[33]

Sub-rule (2) of Rule 6 requires "any Information including sensitive information" to be "disclosed to any third party by an order under the law for the time being in force." This sub-rule does not distinguish between orders issued by a court and those issued by an administrative or quasi-judicial body.

Rule 8 requires body corporates to implement documented security standards such as the international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System".

What is curious about these Rules is that its provisions, particularly those relating to lawful disclosure, appear to go much farther than the limited purpose authorised by Section 43A under which they are framed. Section 43A of the IT Act is intended only to fix liability for the *negligent* disclosure of information by body corporates which results in wrongful loss. It is *not* intended to inaugurate a regime of mandatory disclosure, as the Rules attempt to do. In positively *requiring* body corporates to disclose information upon a mere request by any 'government agency', these Rules attempt to create a parallel, much softer mechanism by which the same information that is dealt with under Sections 69 and 69A and Rules framed under them can be accessed by a far wider range of governmental actors.

Even more curious is the fact that the only legal consequence for the ISP for its negligence in disclosing information to government agencies as stipulated in the Rules is that it exposes itself to possible civil liability from the 'person affected'.[34] Thus, conceivably, if an ISP failed to disclose IP address data of its users to the police at the instance of, say, targets of online financial fraud, they can be sued by the victims of such fraud. With no incentive to assume this ridiculous burden, it is

[33] This is a curious insertion since it begs the question as to the utility of such a statement issued by the requesting agency. What are the sanctions under the IT Act that may be attached to a government agency that betrays this statement? Why not, instead, insert a peremptory prohibition on government agencies from disclosing such information (with the exception, perhaps, of securing conviction of offenders)?

[34] The consequence of disobeying the Rules is that the 'body corporate' is legally deemed not to have observed 'reasonable security practices'. Section 43A penalises such failure if the disclosure causes wrongful loss.

foreseeable that ISPs would hasten to comply with every request for information from a government agency – however whimsically issued.

(3) Intermediary Due Diligence

Section 79 of the IT Act makes intermediaries, including ISPs, liable for third party content hosted or made available by them *unless* they observe 'due diligence', follow prescribed guidelines and disable access to any unlawful content that is brought to their attention.[35] Rules were notified under this Section in April 2011, which defined the 'due diligence' measures they were required to observe.[36]

Accordingly, ISPs are required to forbid users from publishing, uploading or sharing any information that:

(a) belongs to another person and to which the user does not have any right to;
(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, racially or ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatsoever;
(c) harms minors in any way;
(d) infringes any patent, trademark, copyright or other proprietary rights;
(e) violates any law for the time being in force;
(f) deceives or misleads the addressee about the origin of such messages, or communicates any information which is grossly offensive or menacing in nature;
(g) impersonates another person;
(h) contains software viruses or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting any other nation.

[35] Information Technology Act (2000), § 79.

[36] INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES (2011).

Upon being notified by any 'affected person' who objects to such information in writing, the ISP is required to "act within thirty six hours and where applicable, work with [the] user or owner of such information to disable such information."[37]

Further, "when required by lawful order", the ISP, website or any other intermediary:

> shall provide information or any such assistance to Government Agencies that are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

The same attempt at subversion of Sections 69 and 69B, as discussed in the previous sub-section under the Data Protection Rules, is visible here. Failure to observe these 'due diligence' measures – including disclosure of IP address details – would expose ISPs and web services like Google and Facebook to civil liability under Section 79, a risk they would not be likely to or lightly wish to assume.

3. Police Powers of Investigation

Apart from the provisions under the IT Act, to what extent are the police in India empowered under the Code of Criminal Procedure to simply requisition information – including IP addresses of suspects – from ISPs and websites? In the course of routine investigation into other offences, the police have wide powers to summon witnesses, interrogate them and compel production of documents. Can these

[37] The easily-affronted have thus been provisioned with a cheaper, swifter and more decisive means of curtailing free speech, where courts in India might have dithered ponderously instead. Or they might not have. At the time of writing this, an obscure court in Silchar, Assam, issued an ex-parte injunction prohibiting the online publication of a highly-acclaimed biopic about Arindam Chaudhuri – a self-proclaimed 'management guru' who has gained notoriety in India due the questionable nature of a management institute that he runs. The choice of this particular court as the venue to file the suit, rather than one in New Delhi where both the plaintiff and the publisher reside, coupled with Chaudhuri's consistent success in obtaining such plenary gag-orders from this judge against any content he deems unflattering to himself, strongly suggests foul-play. Although this is not a typical case, it does caution against placing too much optimism on supposed judicial restraint and conservativeness. *IIPM's Rs 500-Million Lawsuit against The Caravan*, THE CARAVAN (July 1, 2011), http://caravanmagazine.in/Story/950/IIPM-s-Rs500-million-lawsuit-against-The-Caravan.html.

powers be invoked to obtain IP address information? Are ISPs and websites somehow immune from complying with these requirements?

Section 91 of the Code of Criminal Procedure empowers courts or police officers to call for, by written order, the production of documents or other things that are "necessary or desirable" for the purpose of "any investigation, inquiry, trial or other proceeding under the Code".

Sub-section (3) of this Section, however, limits the application of this power by exempting any "letter, postcard, telegram, or other document or any parcel or thing in the custody of the postal or telegraph authority." Such documents can only be obtained under judicial scrutiny by following a more rigorous procedure laid down in Section 92. Under this Section, it is only if a "District Magistrate, Chief Judicial Magistrate, Court of Session or High Court" is of the opinion that "any document, parcel or thing in the custody of a postal or telegraph authority is...wanted for the purpose of any investigation, inquiry, trial or other proceeding under this Code" that such document, parcel or thing can be required to be delivered to such Magistrate or Court.

However, the same Section empowers lesser courts and officers such as "any other Magistrate, whether Executive or Judicial, or ... any Commissioner of Police or District Superintendent of Police" to require "the postal or telegraph authority, as the case may be ...to cause search to be made for and to detain such document, parcel or thing" pending the order of a higher court.

Section 175 of the Cr.P.C. makes it an offence for a person to intentionally omit to produce a document which he is legally bound to produce. In case the document was to be delivered to a public servant or police officer, such omission is punishable with simple imprisonment of up to 1 month, or with fine up to five hundred rupees, or both. If the document was to be delivered to a Court of Justice, omission could invite simple imprisonment up to 6 months, with or without a fine of one thousand rupees.

In the context of our discussion on IP addresses, the following questions emerge:

1) Are ISPs "telegraph authorities" such that the police are ordinarily prohibited from requisitioning information from them without obtaining orders from a court?

2) Similarly, are webmail and social networking sites "telegraph or postal authorities" such that securing information from them requires following of the special procedure laid down in Section 92?

Section 3(6) of the Indian Telegraph Act, 1885 defines "telegraph authority" as "the Director General of [Posts and Telegraphs], and includes any officer empowered by him to perform all or any of the functions of the telegraph authority under this Act."[38] This would seem to exclude all private sector ISPs from the definition, presumably opening them up to ordinary summons issued under Section 91.

However, Section 3(2) defines a "telegraph officer" to mean "any person employed either permanently or temporarily in connection with a telegraph established, maintained or worked by [the Central Government] *or by a person licensed under this Act*".[39] Under this section, employees of private ISPs such as Airtel would also be regarded as "telegraph officers" and if we can extend this logic, with some interpretative work, the ISPs themselves might be regarded as "telegraph authorities". In the absence of definite rulings by the judiciary on this question, however, the ordinary presumption would be that private ISPs are not "telegraph authorities" and are answerable, like all private companies, to requisitions made under Section 91.

This leaves open the question of whether a government company like BSNL would count as a 'telegraph authority'. If it is, then it would put internet communications conducted through BSNL on a more secure footing than those conducted through other ISPs. As things stand, however, it appears that BSNL seems to be extending its co-operation to the police in tracking mischief online,[40] in the same manner as other ISPs.

---

[38] Indian Telegraph Act (1885), § 3(6).

[39] Indian Telegraph Act (1885), § 3(2).

[40] *See* ALI, *supra* note 9 ("During investigations, the police browsed through several service providers and finally zeroed in on BSNL, which helped them trace the sender's IP address to someone called 'Manoj Gupta' in Gurgaon. A team of policemen were sent to Gurgaon but the personnel found out that Manoj Gupta was [a] fictitious name which the teenager was using in his IP address. The police arrested the accused as well as seized the hardisk [sic] of his personal computer."). *See also* Teresa Rehman, *A Case For Fools?*, TEHELKA (Oct. 10, 2008), http://www.tehelka.com/story_main40.asp?filename=Ws181008case_fools.asp ("The state police reportedly traced the email to the cyber café through its IP address. "We traced the email to a BSNL line. The BSNL has a cell in Bangalore to track such details. They traced the number to that particular cyber café in Shillong," S.B. Singh, IGP (special branch), Meghalaya police told TEHELKA").

The second question is relatively more straightforward. The definition of "post office" in Section 2(k) of the Indian Post Office Act, 1898 restricts its meaning to "the department, established for the purposes of carrying the provisions of this Act into effect and presided over by the Director General [of Posts and Telegraphs]". Despite their primary functions as e-mail providers, it seems unlikely that any magistrate would interpret webmail providers like Hotmail and Google as "postal authorities" so as to be immune from police summonses under Section 91. Such an interpretation would, nevertheless, be in keeping with the spirit of the postal exemptions, since these sections seem to be aimed at requiring judicial oversight before the privacy of communications may be disturbed. It would be fitting for an amendment to be introduced to the Code of Criminal Procedure to update these sections in line with new technological developments.

Before parting with this sub-section, it must be asked whether the procedure under the IT Act or the Code of Criminal Procedure must be followed. Section 81 of the IT Act unequivocally declares that the Act is to have overriding effect "notwithstanding anything inconsistent therewith contained in any other law for the time being in force." This seems to suggest that at least with respect to the interception of electronic communications and obtaining traffic data, the provisions of the Code of Criminal Procedure would be overridden by the procedure laid down by the Rules under the IT Act. The evidence from the practice of the Indian police routinely obtaining IP address from web service providers and ISPs seems to suggest that the IT Act has not been invoked in these transactions. This is a trend that is likely to continue until its legality is questioned in a court of law.

4. Subscriber Contracts with Web Service Providers

In addition to statutory provisions mandating the disclosure of IP address information, such disclosure may also be permissible by the terms under which individual websites provide their services. Two examples would suffice here:

Google's privacy policy which governs its full range of services, from its popular search service to Gmail, as well as the groups and blogging services, states that the company will disclose personal information *inter alia if*:

> [w]e have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable

> governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.[41]

Information collected by Google includes server logs which include the following information: "your web request, your interaction with a service, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser or your account."[42]

Similarly, social networking site Facebook contains an equally expansive 'lawful disclosure' clause in its Privacy Policy,[43] which states that the company will disclose information:

> [t]o respond to legal requests and prevent harm. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.

Information collected by Facebook includes information about the device (computer, mobile phone, etc.), the browser type, the location and IP address, as well as the pages visited.[44]

---

[41] *Privacy Policy*, GOOGLE (Oct. 3, 2010), http://www.google.com/policies/privacy/archive/20101003/.

[42] *Id.*

[43] *Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last visited June 28, 2011).

[44] *Ibid.*

Examples of such clauses abound and it would be fair to assume that almost every corporate website one visits has analogously worded terms of service permitting 'lawful disclosure'. This contractual backdoor negatives any expectation of absolute privacy of IP address details that one might mistakenly have harboured.

Conclusion

IP addresses have proven to be a dependable way for the police in India to track down a range of cyber-criminals – from financial frauds, to vengeful spurned-lovers, to blackmailers and terrorists. The novelty of 'cyber crimes', as well as the relative high-tech ease of their resolution, makes for attractive press and offers an inexpensive way for police departments to accrue some credibility and goodwill for themselves. So long as the police track down *genuine* culprits, the question of privacy violations will necessarily remain suppressed since, in the words of the Supreme Court, "*the protection [of privacy] is not for the guilty citizen against the efforts of the police to vindicate the law*."[45] However, it is the possibility of an increase in egregious cases such as those of Lakshmana Kailash, mentioned above, wrongfully jailed for 50 days on account of a technical error, that reveals the pathologies of the unchecked system of IP address disclosure that prevails today.

Legal regimes in the West have largely been indecisive about whether to characterise the maintenance of IP address logs as handmaids for Orwellian thought-policing, or merely as implements that aid the apprehension of cyber criminals who have no legitimate expectation of privacy. Their laws typically come with procedural safeguards such as mandatory notices to affected persons[46] and judicial review, which greatly mitigate the severity of these disclosures when they do occur.

Far from incorporating such safeguards, the various layers of Indian law create an atmosphere that is intensely hostile to the withholding of such information by ISPs and intermediaries. Overlapping layers of regulation between the Telegraph Act and the IT Act, and the conflict among various Rules under the IT Act have created a climate of such indeterminacy that immediate compliance with even

---

[45] R. M. Malkani v. State of Maharashtra, AIR 1973 SC 157.

[46] *E.g.*, 18 U.S.C. § 2703 (1997) provides for mandatory notice in case of wiretapping with a provision of 'delayed notice' where an 'adverse result' is apprehended such as (A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

the most capricious of information demands by any government agency is the only prudent recourse for ISPs and other intermediaries. The DoT has issued a circular requiring the registration of public and domestic wifi networks to facilitate greater precision in tracking individuals behind IP addresses.[47] For the same purpose, new Cyber Café Rules under the IT Act require extensive registers and logs to be maintained that track the identity of every user and the websites they have visited.[48] And if the full ambitions of the Unique Identity Numbering Scheme and the Centralised Monitoring System are realised, we will shortly be headed for exactly the kind of persistent surveillance society that Orwell wrote so fondly about.

The Indian judiciary, which could have played a counterbalancing role to the legislature's apathy towards privacy and the executive's increasingly totalitarian tendencies, has so far not risen to the challenge. The Supreme Court has repeatedly condoned the obtaining of evidence through illegal means,[49] and this has rendered the requirement of adherence to procedural due process by the police merely optional. This guarantee of judicial inaction in the face of executive illegality will be the biggest stumbling block to the securing of privacy – despite the occasionally good intentions of the legislature.

So, in the absence of a general assurance of privacy of our internet communications, where does one look to for hope? I would venture to suggest that there are four sources of optimism:

a) Notwithstanding the iron determination of the Central Government to install a panoptic communication surveillance system, the realisation and smooth functioning of these technocratic fantasies will depend on the reconfiguration of the relative powers of various

---

[47] Letter from Department of Telecommunications, Ministry of Communications & IT, Government of India to All Internet Service Providers (Feb. 23, 2009), http://www.dot.gov.in/isp/Wi-%20fi%20Direction%20to%20ISP%2023%20Feb%2009.pdf . Internationally, this does not appear to be an uncommon move. *See* Carolyn Thompson, *Innocent Man Accused Of Child Pornography After Neighbor Pirates His WiFi*, HUFFINGTON POST (Apr. 24, 2011, 10:49 AM), http://www.huffingtonpost.com/2011/04/24/unsecured-wifi-child-pornography-innocent_n_852996.html ("In Germany, the country's top criminal court ruled last year that Internet users must secure their wireless connections to prevent others from illegally downloading data. The court said Internet users could be fined up to $126 if a third party takes advantage of their unprotected line, though it stopped short of holding the users responsible for illegal content downloaded by the third party.").

[48] INFORMATION TECHNOLOGY (GUIDELINES FOR CYBER CAFE) RULES (2011).

[49] *See* State Of Maharashtra v. Natwarlal Damodardas Soni, AIR 1980 SC 593.

ministries at the central level – chiefly, the Ministry of Communications and Information Technology and the Home Ministry – and between the Centre and the State. One can rely, one feels, on the unwillingness of various ministries to cede their powers to forestall, or at least delay or diminish the execution of this project. The success of the technology, in other words, is not as much in doubt as is the success of the politics. Privacy will triumph in this 'failure' of politics. I advance this point naively and with only the slightest sense of irony.

b) Another ironic point: I suggest the ingenious and very Indian phenomena of inefficiency and ignorance as robust privacy safeguards. How does one account for the fact that despite heavily worded and repeated invocations of disclosure requirements in the ISP licenses for almost a decade, it was not until December 2010 that the Home Ministry tentatively suggested to ISPs that IP records must be kept for a minimum of six months?[50] This, despite the fact that the ISP license itself requires that such records be kept for one year. How does one explain the unanimous blinking astonishment of the industry at this suggestion, other than they *expected* never to have to implement it*?* How else, similarly, does one explain the fact that the extensive logs that cyber café owners are required to maintain about their clientele are seldom checked?[51] Or that a year after the DoT's circular forbidding open wifi routers, 17% of wireless connections in Mumbai alone were reported 'unsecured'? In India, it seems to be an unstated element of the business climate that one can reliably depend on the non-enforcement of contractual clauses. Sometimes, this inefficiency on the part of the State has inadvertent privacy-preserving effects.

c) The power of the state to rely on IP addresses depends on the availability of global internet behemoths such as Microsoft, Google, Facebook and Yahoo, who are vulnerable to bullying in order to maintain their transnational empires. In each of the success stories mentioned at

---

[50] MCINTYRE, *supra* note 3, at 5.

[51] Shalabh Manocha, *Cops no more interested in checking cyber cafes*, TIMES OF INDIA (Aug. 3, 2009, 1:26 AM), http://articles.timesofindia.indiatimes.com/2009-08-03/lucknow/28172232_1_cyber-cafe-proper-records-ip-address ("The cyber cafe owners claim that the registers which they maintain are seldom checked by the police. "I maintained the records properly which included recording of the name and address of the visitors and a photocopy of their identification proofs but not even once any cop had checked [sic] my records," said Rajeev, a cyber cafe owner in Aliganj. "It is this carelessness on the part of cops that gives those not maintaining proper records to [sic] carry on their business without any fear of the law," he added.").

the start of this paper, IP address details were obtained from one of the big companies named, from which the lesson that emerges is that our ability to retain our anonymity will depend on our ability to find smaller, non-Indian substitutes who have nothing to fear from Indian authorities. In June 2010, for instance, the Cyber Crime Police Station, Bangalore sent a notice under Section 91 of the Cr.P.C. to the manager of BloggerNews.Net (BNN) seeking the IP address and details of a user who had allegedly posted "defamatory comments" on BNN about an Indian company called E2-Labs. The manager of BNN bluntly refused to comply stating: "our policy is not to give out that information, BNN holds people's privacy in high esteem."[52] The lesson here is that in the future, the ability of Indians to preserve their online 'privacy' and freedom of speech will depend on their being able to find sufficiently small overseas clients to host their speech. Conflict of Laws, rather than domestic legislation, is a more reliable guarantor of privacy.

---

[52] Simon Barrett, *Blogger News Censored In India*, BLOGGER NEWS NETWORK (July 12, 2010), http://www.bloggernews.net/124890.