IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 6 2010

Published by
THE LAW AND TECHNOLOGY COMMITTEE
Student Bar Association
National Law School of India University, Bangalore

Faculty Advisor
PROF. T. S. SOMASHEKHAR
Assistant Professor
National Law School of India University, Bangalore

IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 6 2010

BOARD OF ADVISORY EDITORS

INFORMATION ABOUT THE JOURNAL

The Indian Journal of Law and Technology (ISSN 0973-0362) is an academic journal, edited and published annually by students of the National Law School of India University, Bangalore, India. All content carried by the Journal is peer-reviewed except for special comments, student articles and editorial notes. The Journal comprises:

- the Board of Advisory Editors, consisting of professionals and academicians pre-eminent in the field of law and technology, which provides strategic guidance to the Journal;
- the Article Review Board, a panel of external peer-reviewers;
- the Editorial Board, consisting of students of the National Law School of India University, which is responsible for selecting and editing all content as well as contributing occasional editorial notes;
- the Law and Technology Committee, again consisting of students of the National Law School of India University, which publishes the Journal and performs secretarial functions.

INFORMATION FOR CONTRIBUTORS

The Indian Journal of Law and Technology seeks to publish articles, book reviews, comments and essays on topics relating to the interface of law and technology, particularly those with a developing world perspective.

MODE OF SUBMISSION

Submissions can be in electronic form or in hard copy form. However, submissions in electronic form are strongly encouraged in order to expedite the submission review process.

Please address submissions in electronic form to the Chief Editor of the Indian Journal of Law and Technology at "editorialboard@ijlt.in".

Please address submissions in hard copy form to:

The Chief Editor,
Indian Journal of Law and Technology,
National Law School of India University,
Nagarbhavi,
Bangalore 560242,
India.

To facilitate the review of submissions in hard copy form, authors are urged to also provide their submissions in electronic form. However, submissions in hard copy form cannot be returned to the authors through post or other means.

REGULAR SUBMISSION REVIEW

The Journal shall communicate an acknowledgement to all authors shortly after the receipt of their submissions. The preliminary review of the submissions shall be completed within four weeks of receipt in usual circumstances. The submissions that are initially accepted shall be blind–refereed by the Article Review Board. The Journal shall make due efforts to complete the entire peer-review process within a reasonable time frame. The Journal shall notify the authors about the exact status of the peer-review process as required.

EXPEDITED SUBMISSION REVIEW

This option is available to those authors who have received an offer of publication from another journal for their submissions. The authors may request an expedited submission review. However, the decision to grant an expedited submission review shall remain at the discretion of the Editorial Board. Please note that requests for an expedited submission review can only be made in relation to submissions in electronic form. All such requests must be accompanied by the following details:

- Name(s) of the author(s) and contact details;
- Title of the submission;
- Details about the journal(s) which has/have offered to publish the submission;
- Whether the offer is conditional or unconditional and, if the offer is conditional, then what conditions are required to be met for final acceptance;
- The date(s) on which the offer(s) expire(s).

The Journal shall make due efforts to accommodate the existing offer(s) and applicable deadline(s). However, upon an offer of publication pursuant to the expedited submission review, the authors shall have to communicate their decision within five calendar days of the notification of the offer. If there is no response, then the Journal shall have the discretion to withdraw the offer.

SUBMISSION REQUIREMENTS

- All submissions must be accompanied by:
    (1) a covering letter mentioning the name(s) of the author(s), the title of the submission and appropriate contact details.
    (2) the résumé(s)/curriculum vitae(s) of the author(s).
    (3) an abstract of not more than 200 words describing the submission.

- All submissions in electronic form should be made in the Microsoft Word file format (.doc) or in the OpenDocument file format (.odt).
- All text and citations must conform to a comprehensive and uniform system of citation. It is preferred that the system prescribed in THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 18th ed., 2005) or a more recent edition thereof be observed. The Journal employs footnotes as the method of citation.
- No biographical information or references, including the name(s) of the author(s), affiliation(s) and acknowledgements should be included in the text of the submission, the file name or the document properties. All such information can be provided in the covering letter.
- The Journal encourages the use of gender-neutral language in submissions.
- The Journal shall be edited and published according to the orthographical and grammatical rules of Indian English that is based on British English. Therefore, submissions in American English shall be modified accordingly. The Journal encourages authors to use British English in their submissions in order to expedite the editing process.
- The Journal strongly encourages authors to not exceed 30,000 words (inclusive of footnotes) in their submissions.
- The authors are required to obtain written permission for the use of any copyrighted material in the submission and communicate the same to the Journal. The copyrighted material could include tables, charts, graphs, illustrations, photographs, etc. according to applicable laws.

COPYRIGHT

The selected authors shall grant a licence to edit and publish their submissions to the Journal but shall retain the copyright in their submissions. The aforementioned licence shall be modelled as per a standard author agreement provided by the Journal to the selected authors.

DISCLAIMER

The opinions expressed in this journal are those of the respective authors and not of the Journal or other persons associated with it.

PERMISSIONS

Please contact the Chief Editor of the Indian Journal of Law and Technology for permission to reprint material published in the Indian Journal of Law and Technology.

SUBSCRIPTION INFORMATION

The following procedure should be followed in relation to subscription requests.

- Send a cheque or a demand draft in the name of the "Registrar, National Law School of India University". Send a covering letter accompanying the cheque or the demand draft stating requisite contact details including postal address, telephone number and e-mail address.
- Send an e-mail to "editorialboard@ijlt.in" and "library@nls.ac.in" confirming the subscription request and the subscription payment. The e-mail should also provide the contact details mentioned hereinabove.
- If the subscription payment is received then the subscription shall be confirmed through an e-mail. If no request for back-issues is made, then the subscription shall commence from the forthcoming issue.
- Contact the Managing Editor at "editorialboard@ijlt.in" for inquiries and updates.

ANNUAL SUBSCRIPTION RATES (POSTAGE INCLUDED)

Indian Subscribers

	One Year	Two Years	Three Years
Students	INR100	INR200	INR300
Others	INR200	INR400	INR600

International Subscribers

	One Year	Two Years	Three Years
Students	US$25	US$45	US$55
Others	US$35	US$60	US$80

Please visit the website of the Indian Journal of Law and Technology at "http://www.ijlt.in" to get additional information and to access the archives of previous volumes.

IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 6 2010

CONTENTS

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 6, 2010

JURISDICTIONAL ISSUES IN CYBERSPACE

Justice S. Muralidhar[*]

I

INTRODUCTION

With the advent of the internet and the transmission of information and transacting of business across borders, a host of issues have cropped up on the legal front. This article proposes to deal with only one such major issue – that of jurisdiction of the courts to deal with intellectual property rights (IPR) disputes arising out of commercial transactions on the internet. Within the fairly broad field of IPR, the focus will be on trademark disputes, as that is one area where the major developments have taken place.

The traditional approach to jurisdiction invites a court to ask whether it has the territorial, pecuniary, or subject matter jurisdiction to entertain the case brought before it. With the internet, the question of 'territorial' jurisdiction gets complicated largely on account of the fact that the internet is borderless. Therefore, while there are no borders between one region and the other within a country there are no borders even between countries. The computer as a physical object within which information is stored has given way to 'cyberspace' where information is held and transmitted to and from the 'web.' So where is this 'place' where the information is 'held'?

There is a clear geographical limitation to IP rights. Where registration is granted, say, of a trademark or a patent or copyright, it operates to prevent others from infringing those rights within the territory of the state where the registration is granted. It prevents even those outside the territory of the state from infringing those rights within the territory. The statutory law, as enforced by courts of the territory, accords due recognition to this system. Outside of infringement actions, courts have in passing off actions sought to protect trademarks and trade names of users within the territory to the exclusion of those seeking to pass off their goods as that of the holder of the right. Where the goods are tangible and bought and sold within the territory, enforcement of

[*] Judge, High Court of Delhi. I wish to thank Apurv Sarvaria, my Law Researcher, for his assistance in sourcing the background material used in this article.

such law is not a problematic issue. However, a holder of IP rights accorded protection in a state cannot enforce those rights in a foreign state within whose territory the infringer is located and the laws of which do not acknowledge the activity to be an infringement. Further, all of the above assumptions change in the context of transactions over the internet and even more so when the products or services themselves are not in physical form but in a virtual world. Also, in a borderless cyber world, the products and services can be transmitted easily across countries in a flash. It then compounds the problem as the following example shows.

The product is a copyrighted song in the MP3 digital format. The transaction can begin with the 'uploading' of the product in one territory, being held on a server in another, being advertised for sale on the website of a service provider in a third country, being 'bought' by a click and pay service hosted in yet another territory, and finally 'downloaded' in another territory. The complete transaction turns out to be a sale of a pirated product which *per se* is an infringement of the copyright in the song in question. Does the court in each of these territories have jurisdiction to entertain the dispute?

The notion of jurisdiction is rooted in territoriality from the point of view of both the court which can properly assert jurisdiction and from the point of view of the law that should be applied while deciding the dispute.

A caveat at this stage would be in order. What is applicable to international transactions involving the internet, could well apply to 'domestic' transactions as well. The law as developed in the USA has had to reckon with both situations, i.e., internet transactions across countries and those across states. The enforcement issues would of course be more complex when it comes to international transactions. However, the principles applied by courts to assert or negate jurisdiction in either instance have remained more or less similar. The *Yahoo!* case[1] is one instance of this and will be discussed elaborately later as it throws up several dimensions. In the *Banyan Tree Holding* case,[2] the Delhi High Court was dealing with an inter-state issue of jurisdiction and not an international dispute. Interestingly, the plaintiff was a foreign company which had invoked the jurisdiction of an Indian court to seek an injunction against the alleged violator of its trademark. The court by and

[1] Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000 and November 22, 2000, No RG:00/0538 (Fr.).

[2] Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy & Anr., CS(OS) 894/2008 (High Court of Delhi, 23rd November 2009) (India).

large followed the development of common law in the USA, the UK and some other Commonwealth countries. An indigenous law is yet to be developed for India.

The inability of countries to effectively regulate the transactions on the internet originating or ending within their territories stems from the nature of the technology itself. While countries can seek to enforce their respective laws within their physical, geographical and political spaces delineated on an atlas, a borderless cyberworld, controlled by technology that is constantly changing, throws up several challenges. Even while it was thought that one could fix the physical location of the computer from where the transaction originates and the one where it ends, that too can be bypassed or 'masked' by technology. Legal scholar Wendy Adams sums up the problem as thus:

> Internet, as a communications system, has been designed to be largely indifferent to the physical location of its component parts. The closest equivalent to a physical location in Internet communications (as opposed to the physical infrastructure, which is readily identifiable as existing in a given geographical location) is an Internet Protocol (IP) address, a 32-bit number providing the necessary information for routing communications between computers attached to the network. The sending computer needs to know the 32-bit address of the receiving computer in order for communication to take place; it does not need to know the street address, city or country of the building in which the receiving computer is physically located. This fundamental incompatibility between legal governance as a function of geopolitical territory, and network governance as a function of IP addressing, makes it difficult (although not impossible) to impose local limitations on the global dissemination of information.[3]

On the second question of the applicable law, the principle invoked is of 'sovereign equality within international law.' In the more traditional mode of dispute resolution involving two countries, resort is had to public international law. Where the dispute is between entities and persons in different countries, the sphere of private international law is meant to find a solution. In the area of IPR violations and infringement across borders, there is yet to develop a universal law. The TRIPS Agreement is not the 'uniform' law in the area. Resort is still to be had to private international law. Wendy Adams explains:

> In circumstances of regulatory diversity involving geographically complex facts, domestic courts must apply the law of one state to the exclusion of all others,

[3] Wendy A. Adams, *Intellectual Property Infringement in Global Networks: The Implications of Protection Ahead of the Curve,* 10 INT'L J.L. & INFO. TECH. 71 (2002).

> notwithstanding that each state can rightfully claim that some portion of the impugned activity has taken place within its territorial borders. In choosing the law of a single State to govern the transaction or dispute, domestic courts are effectively deeming the activity to have occurred within that state. The foundational principle of **sovereign equality within international law** requires this legal fiction, as a State's authority to prescribe or enforce its laws does not extend beyond its territorial jurisdiction. Such questions of jurisdiction are inevitable in disputes involving on-line activity, as **the lack of territorial precision in an on-line environment necessarily leads to geographically complex facts. Accordingly, domestic courts addressing these disputes will first have to localise the transaction prior to assuming jurisdiction.** At issue is whether domestic courts will develop localisation processes which have unanticipated spillover effects in the international trade regime in relation to the benefits and burdens allocated under the TRIPS Agreement.[4] (Emphasis Supplied)

The need for local courts to 'localise' the transaction has posed a challenge that has generated a variety of responses which are analysed in the following section.

II

This part examines the efforts made by courts in different countries to 'localise' transactions in IPR disputes in the process of exercising personal jurisdiction over defendants located outside their territories. It traces the development of the law first in the USA, through the 'minimum contacts' test, the 'purposeful availment' test, the *Zippo* 'sliding scale' test and the 'effects' tests. It discusses the difficulties with each of these tests in their application to cases. Thereafter the development of the law in the UK, Canada, Australia and India is discussed.

THE USA

Minimum Contacts Test

In *International Shoe Co. v. Washington*,[5] a two-part test for determining jurisdiction of the forum court over a defendant not residing or carrying on business within its jurisdiction was evolved. It was held that in such instance the plaintiff had to show that the defendant has sufficient 'minimum contacts' in the forum state. In other words, the defendant must have purposefully directed its activities towards the forum state or otherwise 'purposefully availed' of the privilege of conducting activities in the forum state. Further, the forum court had to be satisfied that exercising jurisdiction would comport with the traditional notions of fair play and substantial justice. The

[4] *Id.*
[5] 326 U.S. 340 (1945).

minimum contacts test in *International Shoe* has been understood as to have performed "two related, but distinguishable, functions."[6] The first was to protect the defendant from the burden of litigating in a distant or inconvenient forum.[7] The second was to ensure that the states do not "reach out beyond the limits imposed on them by their status as coequal sovereigns in a federal system."[8]

Michael Geist points out that:

> In many jurisdictions, the litmus test for determining whether assertion of jurisdiction is appropriate involves analyzing whether jurisdiction is reasonable under the circumstances, with courts in the United States and Canada regularly relying on a reasonableness standard as their guide. In the United States, the reasonableness standard is couched in terms of 'minimum contacts,' while in Canada the language of choice is 'real and substantial connection.' Although these terms necessitate somewhat different analyses, the core principle remains the same - the appropriateness of asserting jurisdiction depends upon whether the parties themselves would think it reasonable to do so.[9]

He explains that: "...a foreseeability metric lies at the heart of the reasonableness standard. This metric dictates that a party should only be hauled into a foreign court where it was foreseeable that such an eventuality might occur."[10] This test, as will be seen later, appears to have greater practical relevance in deciding jurisdictional issues than other tests that have been subsequently evolved.

Recently, the Court of Appeals for the Ninth Circuit in *Boschetto v. Hansing*,[11] while rejecting the 'sliding scale' test (laid down in the *Zippo* case[12] which is discussed later) has followed the minimum contacts test. However, the traditional minimum contacts approach is limited to the category of cases to which *International Shoe* most directly applied, i.e., long-range commercial transactions. It would not be applicable to cases involving remote torts or goods that were moved

---

[6] World-Wide Volkswagen v. Woodson, 444 U.S. 286, 291-92 (1980).
[7] *Id.*
[8] *Supra* note 6.
[9] Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1356 (2001).
[10] *Id.*
[11] 539 F.3d 1011 (9th Cir. 2008).
[12] Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D.Pa. 1997).

after purchase[13] and cases dealing with internet defamation and other non-commercial transaction cases.

Purposeful Availment Test

The US Supreme Court's focus on purposeful conduct of the defendant emerged in *Hanson v. Denckla*.[14] The facts here were that a Florida court asserted jurisdiction over a Delaware trust company, in an action challenging a Florida resident's appointment of property of which the Delaware company was trustee. The settlor had after the creation of the trust moved from Pennsylvania to Florida. However, the trust company had not solicited or conducted business in Florida other than routine correspondence with the settlor. Holding that the Florida court did not have jurisdiction, the US Supreme Court held that the trust company had not purposefully undertaken to conduct business in Florida. It was connected with the state only because the settlor unilaterally moved to Florida subsequent to the contractual relationship being established.

In *World-Wide Volkswagen Corp. v. Woodson*,[15] an automobile was involved in an accident while it was being driven by the purchasers through Oklahoma. The question was whether the wholesaler and retailer, both located in New York, could be made amenable to the jurisdiction of the Oklahoma court where a product liability claim was filed. In holding that the wholesaler and retailer were not subject to personal jurisdiction there, the US Supreme Court pointed out that the defendants had not undertaken to conduct any business in Oklahoma. Their only connection with that state arose as a result of the 'unilateral activity' of the purchasers driving the car there. The Court explained that the foreseeability that an automobile might be taken to Oklahoma was not relevant. According to it what was relevant was the foreseeability "that the defendant's conduct and connection with the forum state are such that he should reasonably anticipate being hauled into court there."[16]

In *Burger King Corp v. Rudzewicz*,[17] the Supreme Court held that the defendant did not have to be physically present within the jurisdiction of the forum court and that the forum court may exercise jurisdiction over a non-resident where an alleged injury arises out of or relates to actions by the

[13] *See* Calder v. Jones, 465 U.S. 783 (1984) *and* World-Wide Volkswagen.
[14] 357 U.S. 235 (1958).
[15] 444 U.S. 286 (1980).
[16] *Id.* at 297.
[17] 471 U.S. 462 (1985).

defendant himself that are 'purposefully directed' towards residents of the forum state.[18] It was held that 'purposeful availment' would not result from 'random' or 'fortuitous' contacts by the defendant in the forum state. It requires the plaintiff to show that such contracts resulted from the "actions by the defendant himself that created a substantial connection with the forum state."[19] He must have engaged in 'significant activities' within the forum state or created 'continuing obligations' between himself and the residents of the forum state. It was held on facts that the twenty year relationship that the defendant had with the plaintiff "reinforced his deliberate affiliation with the forum state and the reasonable foreseeability of litigation there."[20]

In *Asahi Metal Industry v. Superior Court*,[21] the US Supreme Court reversed the decision of the State Supreme Court and held that exercise of personal jurisdiction over the Japanese company would be unreasonable and unfair, and so constitute a violation of the Due Process Clause. Furthermore, it was held that 'the mere placement of a product into the stream of commerce' was not an act 'purposefully directed towards the forum state' and so it would not result in a 'substantial connection' between the defendant and the forum state as required to support a finding of minimum contacts.[22]

The US Supreme Court remained divided (4:4:1) on whether the Japanese supplier of valve assemblies, which were incorporated into tyre tubes by a Taiwanese company and subsequently distributed by that company in California, had purposefully availed itself of the benefits of doing business in California. Justice O'Connor, joined by three other judges, held that something more than the defendant's awareness that its valve assembly might be swept into the state in the 'stream of commerce' and cause an injury there must have been shown.[23] It was held that Asahi should be shown to have engaged in some act 'purposefully directed toward the forum state,' such as designing the product for the forum state, advertising or providing customer service there, or enlisting a distributor to serve the state.[24] Justice Stevens concurred but for separate reasons. Justice Brennan dissented along with three judges on the other hand. The dissenting judges found that Asahi had made 'regular and extensive' sales of component parts to a manufacturer which in

[18] *Id.* at 471-478.
[19] *Supra* note 17, at 475.
[20] *Supra* note 17, at 482.
[21] 480 U.S. 102 (1987).
[22] *Id.* at 108-13 & 116.
[23] *Supra* note 21, at 112.
[24] *Supra* note 21, at 112.

turn was selling the manufactured product in California. According to the dissenting judges, the fact that Asahi knew this was sufficient to make it amenable to the Californian court's jurisdiction. It observed:

> The stream of commerce refers not to unpredictable currents or eddies, but to the regular and anticipated flow of products from manufacture to distribution to retail sale. As long as a participant in this process is aware that the final product is being marketed in the forum state, the possibility of a lawsuit there cannot come as a surprise.[25]

The difference in the respective approaches was precisely this. The majority opinion rendered by Justice O'Connor required Asahi to have engaged in conduct indicating 'intent or purpose to serve the market' whereas for the dissenting judges it was sufficient that the defendant had placed its product in the 'stream of commerce.' The dissenting judges also emphasised on the presumed awareness of Asahi that the product would be 'swept into the state of California' and so in such circumstances 'the possibility of a lawsuit there could not come as a surprise' to the defendant.

In *Inset Systems Inc. v. Instruction Set Inc.*,[26] the defendant had displayed on its website used for advertising its goods and services, a toll-free telephone number '1–800–US–INSET.' The plaintiff, a company in Connecticut brought an infringement action against the defendant in a court in Connecticut, which in any event had a long arm statute. The District court held that the defendant had:

> purposefully availed itself of doing business in Connecticut because it directed its advertising activities via the Internet sites and toll-free number toward the State of Connecticut (and all states); Internet sites and toll-free numbers are designed to communicate with people and their businesses in every state; an Internet advertisement could reach as many as 10,000 Internet users within Connecticut alone; and once posted on the Internet, an advertisement is continuously available to any Internet user.[27]

However, the approach in *Bensusan Restaurant Corp. v. King*,[28] was different although New York too had a long arm statute. The defendant therein had a small jazz club known as 'The Blue Note' in Columbia, Missouri and created a general access web-page giving information about the said club as well as a calendar of events and ticketing information. In order to buy tickets, prospective

---

[25] *Supra* note 21, at 117 (Brennan, J., dissenting).
[26] 937 F. Supp. 161 (D. Conn. 1996).
[27] *Id.* at 165.
[28] 937 F. Supp. 295 (S.D.N.Y. 1996).

customers had to use ticket outlets in Columbia. Bensusan (the plaintiff therein) was a New York corporation that owned 'The Blue Note,' a popular jazz club in the heart of Greenwich Village in New York. It also owned the rights to the 'The Blue Note' trademark. It accordingly sued the defendant for trademark infringement in New York. It was noticed that New York had a long arm statute. However, the New York court held that the defendant had not done anything to purposefully avail himself of the benefits of the forum. Like numerous others, the defendant had "simply created a web site and permitted anyone who could find it to access it. **Creating a site, like placing a product into the stream of commerce, may be felt nationwide or even worldwide but, without more, it is not an act purposefully directed towards the forum state.**"[29] (Emphasis Supplied)

In *Ballard v. Savage*,[30] it was explained that the expression 'purposefully availed' meant that "the defendant has taken deliberate action within the forum state or if he has created continuing obligations to forum residents."[31] It was further explained that "it was not required that a defendant be physically present within, or have physical contacts with the forum, provided that his efforts are purposefully directed toward forum residents."[32] In *CompuServe, Inc. v. Patterson*,[33] it was found that the defendant had chosen to transmit its products from Texas to CompuServe's system, and that system provided access to his software to others to whom he advertised and sold his product. It was held that Patterson had "purposefully availed himself of the privilege of doing business."[34]

In *Maritz, Inc. v. CyberGold Inc.*,[35] where internet surfers who came across its website were encouraged by the defendant CyberGold to add their e-mail address to a mailing list that basically subscribed the user to the service, it was held that the defendant had obtained the website for the purpose of and in anticipation that internet users will access CyberGold's website and eventually sign up on CyberGold's mailing list. Therefore, although CyberGold claimed that its website was a passive one, it was held that through its website, "CyberGold has consciously decided to transmit

---

[29] *Id.* at 301.
[30] 65 F.3d 1495 (9th Cir. 1995).
[31] *Id.*
[32] *Supra* note 30, at 1498.
[33] 89 F.3d 1257 (6th Cir. 1996).
[34] *Id.* at 1266.
[35] 947 F. Supp. 1328 (E.D. Mo. 1996).

advertising information to all internet users, knowing that such information will be transmitted globally."[36]

In *Neogen Corp. v. Neo Gen Screening, Inc.*,[37] the Court of Appeals held that the purposeful availment requirement is satisfied if the web site is interactive to such a degree that reveals a specifically intended interaction with residents of the state. In that case, the plaintiff (Neogen), a Michigan Corporation, was in the business of developing and marketing a range of health care, food, and animal-related products and services, including certain diagnostic test kits. It filed a suit in the Michigan District Courts alleging, *inter alia*, trademark infringement against the defendant (Neo Gen Screening/NGS), a Pennsylvania Corporation performing diagnostic testing of blood samples from newborn infants. The District Court dismissed the suit for lack of personal jurisdiction. The Court of Appeals held that the maintenance of the defendant's website, in and of itself, does not constitute purposeful availment of the privilege of acting in Michigan. It observed that: "the level of contact with a state that occurs simply from the fact of a website's availability on the Internet is therefore an attenuated contact that falls short of purposeful availment."[38] However, the Court in that case did not decide the question of whether the defendant's website alone would be sufficient to sustain personal jurisdiction in the forum state as it held that the website should be considered alongside other interactions with Michigan residents. It also observed that when potential customers from Michigan had contacted NGS to purchase its services, NGS had welcomed their individual business on a regular basis. The Court further observed that "although customers from Michigan contacted NGS, and not the other way around, NGS could not mail test results to and accept payment from customers with Michigan addresses **without intentionally choosing to conduct business in Michigan**."[39] (Emphasis Supplied) It was in this context that the Court of Appeals reversed the finding of the District Court and remanded the matter.

In *Cybersell, Inc. v. Cybersell. Inc.*,[40] the facts were that an Arizona Corporation that advertised for commercial services over the internet under the service mark 'Cybersell', brought an infringement action against a Florida Corporation that offered web-page construction services over the internet. As part of its marketing effort, the Florida Corporation created a web-page that had a logo at the top consisting of 'CyberSell' over a depiction of the planet earth, with the caption underneath

---

[36] *Id.* at 1333.
[37] 282 F.3d 883, 890 (6th Cir. 2002).
[38] *Id.* at 892.
[39] *Supra* note 37, at 892.
[40] 130 F.3d 414 (9th Cir. 1997).

'Professional Services for the World Wide Web' with a local telephone number and a hypertext link allowing the internet surfer to introduce herself. That link invited a company not on the web but interested in getting on the web to e-mail the Florida Corporation for further information. Arizona had a long arm statute that permitted a court to exercise personal jurisdiction over parties whether found within or outside the state to the maximum extent permitted by the court in United States. The Court referred to the decision of the Arizona Supreme Court in *Uberti v. Leonardo*,[41] in which it was held that Arizona will exert personal jurisdiction over a non-resident litigant to the maximum extent allowed by the federal constitution. The Arizona Court of Appeals adopted a three part test to determine whether the district court could exercise specific jurisdiction over the non-resident defendant: (1) the non-resident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections; (2) the claim must be one which arises out of the results from the defendant's forum-related activities; and (3) exercise of jurisdiction must be reasonable.[42] It was held by the Court of Appeals that all that Cybersell FL (the Florida Corporation) had done was to:

> post an essentially passive home page on the web, using the name 'CyberSell,' which Cybersell AZ (the Arizona Corporation) was in the process of registering as a federal service mark. While there is no question that anyone, anywhere could access that home page and thereby learn about the services offered, we cannot see how from that fact alone it can be inferred that Cybersell FL deliberately directed its merchandising efforts toward Arizona residents.[43]

It was further noticed that: "the interactivity of its web page is limited to receiving the browser's name and address and an indication of interest-signing up for the service is not an option, nor did anyone from Arizona do so. No money changed hands on the Internet from (or through) Arizona."[44] It was held that Cybersell FL's contacts were insufficient to establish 'purposeful availment.'

Three years later in *Bancroft & Masters Inc. v. Augusta National Inc.*[45] the Circuit Court applied the *Calder* 'effects' test in a trademark dilution and infringement case and upheld jurisdiction. The

---

[41] 181 Ariz. 565, *cert. denied*, 116 S. Ct. 273 (1995).
[42] *Id.* at 570.
[43] *Supra* note 40, at 419.
[44] *Supra* note 40, at 419.
[45] 223 F.3d 1082 (9th Cir. 2000).

plaintiff, a California computer services company, had been granted registration of the domain name 'masters.com' by Network Solutions Inc. (NSI). The defendant Augusta National Inc. (ANI) was a Georgia golf club that held several registrations for 'masters' and a domain name 'masters.org' served a cease-and-desist notice on NSI in California. The plaintiff then responded by filing a suit in California for a declaration that its domain name did not infringe ANI's trademark. The court upheld the exercise of personal jurisdiction over ANI since by serving the notice on NSI in California, ANI 'had expressly aimed' its activity at California.

The Zippo 'sliding scale' test

An extension of the purposeful availment test was attempted in *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*[46] The plaintiff Zippo Manufacturing was a Pennsylvania corporation making cigarette lighters. The defendant was a California corporation operating an internet website and an internet news service. It had offices only in California. Viewers who were residents of other states had to go to the website in order to subscribe for the defendant's news service by filling out an online application. Payment was made by credit card over the internet or telephone. Around 3000 of the defendant's subscribers were residents of Pennsylvania who had contracted to receive the defendant's service by visiting its website and filling out the online application. Additionally the defendant had entered into agreements with seven internet access providers in Pennsylvania to permit their subscribers to access the defendant's news service. The defendant was sued in a Pennsylvania court for trademark dilution, infringement and false designation. After discussing the development of the law till then, the District Court first observed that:

> The Constitutional limitations on the exercise of personal jurisdiction differ depending upon whether a court seeks to exercise general or specific jurisdiction over a non-resident defendant (Mellon, 960 F.2d at 1221.). General jurisdiction permits a court to exercise personal jurisdiction over a non-resident defendant for non-forum related activities when the defendant has engaged in 'systematic and continuous' activities in the forum state (Helicopteos Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408.). In the absence of general jurisdiction, **specific jurisdiction permits a court to exercise personal jurisdiction over a non-resident defendant for forum-related activities where the relationship between the defendant and the forum falls within the 'minimum contacts' framework of International Shoe Co. v. Washington**, 326 U.S. 310 and its progeny, Mellon, 960 F.2d at 1221.[47] (Emphasis Supplied)

[46] 952 F. Supp. 1119 (W.D. Pa. 1997).
[47] *Id.* at 1122.

The *Zippo* court then noted that:

> a three pronged test has emerged for determining whether the exercise of specific personal jurisdiction over a non-resident defendant is appropriate: (1) the defendant must have sufficient 'minimum contacts' with the forum state, (2) the claim asserted against the defendant must arise out of those contacts, and (3) the exercise of jurisdiction must be reasonable.[48]

The court in *Zippo* classified websites as (i) passive, (ii) interactive and (iii) integral to the defendant's business. On facts it was found that the defendant's website was an interactive one. Accordingly it was held that the court had jurisdiction to try the suit. The *Zippo* court's observation that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the internet has been compared by that court to a 'sliding scale.'

In the Court's words:

> At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site, which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.[49]

Zippo was welcomed by courts as offering a balance between a lawless internet and an excessively-regulated one. While an owner of a passive website could not be expected to foresee being sued in multiple jurisdictions worldwide, the owner of an interactive one should expect such an outcome. Also, it tacitly approved the protection of local consumers' interests by local courts applying the local law.

---

[48] *Supra* note 46, at 1122-23.

[49] *Supra* note 46.

Soon, however, problems surfaced in applying the *Zippo* sliding scale test in terms of which the assertion of a court's jurisdiction depended upon the 'level of interactivity and commercial nature of the exchange of information' as a result of the use of the website. The courts have been finding it problematic in determining the degree of interactivity that should suffice for jurisdiction to be attracted. Mere ability to exchange files with users through the internet has been held not to be sufficiently 'interactive' for the forum court to assume jurisdiction.[50]

In *Millennium Enterprises Inc. v. Millennium Music L.P.*,[51] the Oregon district court declined to exercise jurisdiction over a South Carolina corporation that sold products both offline and on the web. The court felt that 'something more' than merely showing that the website was interactive was required. The defendant should be shown to have consummated some transaction within Oregon and to have made 'deliberate and repeated contacts' with Oregon through the website so that it could be held that they ought to have anticipated being hauled into an Oregon court.[52]

In *People Solutions v. People Solutions*,[53] although it was possible for customers visiting the defendant's website to download information, obtain product brochures and order products online, the court refused to assert jurisdiction since the plaintiff failed to show that defendant had sold its products or contracted for services with any person in the forum state through the website. Again in *Mink v. AAAA Development*,[54] although the defendant's website offered printable mail-in order forms that could be downloaded, provided a toll-free number, a mailing and an e-mail address, the forum court declined to exercise jurisdiction since in fact no orders were placed using the website.

In *Winfield Collection v. McCauley*,[55] the website provided an interactive mechanism of doing online business and the plaintiff showed that auction sales were conducted over the net with bidders in Michigan. Nevertheless jurisdiction was declined because the defendant was not shown as "actively and intentionally doing business with customers in Michigan." It was held that the form of online sale made it impossible for the defendant's website to target the users of any particular state and therefore other than the court of the state where the principal place of the business of the

---

[50] *See* Desktop Technologies v. Colourworks Reproduction & Designs Inc., 1999 WL 98572 (E.D. Pa. 1999).
[51] 33 F. Supp. 2d 907 (D. Or. 1999).
[52] *Id.* at 910.
[53] 2000 WL 1030619 (N.D. Tex. 2000).
[54] 190 F.3d 333 (5th Cir. 1999).
[55] 105 F. Supp. 2d 746 (E.D. Mich. 2000).

defendant was located, other state courts could not exercise jurisdiction. Since over the years, most websites are interactive to some degree, there has been a shift from examining whether the website is *per se* passive or active to examining the nature of the activity performed using the interactive website.

Zippo has been criticised as being ineffective in lending legal certainty in the face of ever-changing technology which has witnessed a shift from the use of passive websites to those that are either partly or wholly interactive. If the test were to be static irrespective of the changes in technology, then it would become irrelevant if a majority of the websites answered the definition of an interactive website. That would result in a 'chilling effect' on international commerce of which the internet is a major vehicle. It would then fail to provide the balance between the interests of consumers and those of producers and marketers.

The Effects Test and 'Intentional targeting'

The difficulty experienced with the application of the *Zippo* sliding scale test has paved the way for application of the 'effects' test. The courts have thus moved from a 'subjective territoriality' test[56] to an 'objective territoriality' or 'effects' test in which the forum court will exercise jurisdiction if it is shown that effects of the defendant's website are felt in the forum state. In other words it must have resulted in some harm or injury to the plaintiff within the territory of the forum state. Since some effect of a website is bound to be felt in several jurisdictions given the nature of the internet, courts have adopted a 'tighter' version of the 'effects' test, which is 'intentional targeting.'

The 'effects' test was first evolved in *Calder v. Jones*.[57] The plaintiff therein was a resident of California who commenced a libel action in a California court against the National Enquirer based on an article that it printed and circulated in California. Apart from the Enquirer and its local distribution company, its editor and the author of the article were all in Florida. Affirming the assertion by the California court of personal jurisdiction over the defendants, the Supreme Court held:

> The allegedly libelous story concerned the California activities of a California resident. It impugned the professionalism of an entertainer whose television career was centred in California. The article was drawn from California sources, and the

[56] That a court will regulate an activity only if it is shown having originated in its territory – exemplified by the decision in *Louis Feraud Int'l SARL v. Viewfinder Inc.*, 406 F. Supp. 2d 274 (S.D.N.Y. 2005).
[57] 465 U.S. 783 (1984).

> brunt of the harm, in terms both of respondent's emotional distress and the injury to her professional reputation, was suffered in California. In sum, California is the focal point both of the story and of the harm suffered. Jurisdiction over petitioners is therefore proper in California based on the 'effects' of their Florida conduct in California.[58]

On facts it was held that the author and editor 'expressly aimed' their tortuous actions at California and that they knew that the article would have a devastating impact on the respondent and that they should have reasonably anticipated that the brunt of that injury would be reasonably felt by the defendant in the state in which she lived and worked.

The court went on to observe:

> Petitioners are not charged with mere untargeted negligence. Rather, their intentional, and allegedly tortuous, actions were expressly aimed at California. Petitioner South wrote and petitioner Calder edited an article that they knew would have a potentially devastating impact upon respondent. And they knew that the brunt of that injury would be felt by respondent in the State in which she lives and works and in which the National Enquirer has its largest circulation. Under the circumstances, petitioners must 'reasonably anticipate being hauled into court there' to answer for the truth of the statements made in their article...[59]

Yahoo! Case

The effects test propounded in *Calder* has been applied with mixed results. One of the most discussed decisions of a French court where the effects doctrine was applied is the *Yahoo!* case.[60] A French Jew while surfing on the net came across Nazi memorabilia being offered for sale on a web page hosted by Yahoo!. The offering of Nazi memorabilia for sale was an offence under the French penal law. Although the website of Yahoo! France did not host a similar web page, it could be viewed on the Yahoo! website hosted from the US by anyone in France. LICRA, an organization fighting racism and anti-Semitism, and the Union of Jewish students in France (UJEF) sued Yahoo! and Yahoo! France in the courts in France. The French court ordered Yahoo! to block access to its US website from France, in order to prevent internet users in France from accessing the objectionable items offered for auction sale on that site. It found that this was technologically feasible through a series of devices for which it examined experts. It thus rejected Yahoo!'s argument that the French court's order was not capable of being implemented beyond the borders

---

[58] *Id.* at 788.

[59] *Supra* note 57, at 789-90.

[60] Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000 and November 22, 2000, No RG:00/0538 (Fr.).

of France. The French court essentially applied the effects test to assert jurisdiction. It held that by permitting internet users in France to participate in the sale of such objects, Yahoo! had committed a wrong within the territory of France. Although the website was capable of being viewed from anywhere in the world, the French court concluded that it had caused harm to the two claimants located in France. The mere possibility of downloading the objectionable information did not alone determine the question of jurisdiction. The French court also considered the effect it would have on the public at large in France who could access Yahoo!'s website and who were targeted. Thus the court concluded from the fact that Yahoo! displayed advertisements in French to visitors at the US based server and that Yahoo! France provided a link to the US based Yahoo! server that Yahoo! did intend its services to reach persons in France and also intended to profit from the visitors from France to its US based website.

While courts have more readily applied the effects test in defamation cases,[61] there have been problems in its application to trademark infringement cases. For instance, the Court of Appeals in *Cybersell* held that the 'effects' test did not apply with the same force to Cybersell AZ as it would to an individual, because a corporation does not suffer localised harm in a specific geographic location in the same manner as an individual. Cybersell FL's web page simply was not aimed intentionally at Arizona knowing that harm was likely to be caused there to Cybersell AZ. In *Digital Equipment Corp. v. Alta Vista Technology*,[62] the plaintiff, a Massachusetts company sued the defendant which was its licensee alleging infringement of its mark. Although the defendant argued that it had structured its affairs to avoid the forum state, the court found that the defendant's use of its website to infringe the plaintiff's mark did have effects in the forum state and its purpose may be said to be targeting the forum state and its citizens. In *Nissan Motor Co. v. Nissan Computer Corp*.[63] although the defendant did not sell goods to its consumers on its websites (which were registered under the domain names 'nissan.com' and 'nissan.net') it had intentionally changed the content of its website to exploit the goodwill of the plaintiff by profiting from the confusion created among the consumers. It was therefore held to have "deliberately and substantially directed its activity toward the forum state."[64]

---

[61] *See* Remick v. Manfredy, 238 F.3d 248 (3d Cir. 2001); Noonan v. Winston Comp., 135 F.3d 85, 91 (1st Cir. 1998); Revell v. Lidov, 317 F.3d 467 (5th Cir. 2002).
[62] 969 F. Supp. 456 (D. Mass. 1997).
[63] 89 F. Supp. 2d 1154 (C.D. Cal. 2000).
[64] *Id.* at 1159.

It is pointed out that in developing criteria to be used in determining whether a website has targeted the forum state, care must be taken to ensure that it must be technology neutral in the sense that it will remain relevant even as new technologies emerge. Furthermore, the criteria must not display any bias towards either consumers, who would seek to apply the law governing the destination of the product, or producers who seek to apply the law of the place of origin of the goods. Further, as Michael Geist points out, the real question would be whether the targeting of a specific jurisdiction was foreseeable.

This in turn depends on three factors:

> To identify the appropriate criteria for a targeting test, we must ultimately return to the core jurisdictional principle – foreseeability. Foreseeability should not be based on a passive versus active website matrix. Rather, an effective targeting test requires an assessment of whether the targeting of a specific jurisdiction was itself foreseeable. Foreseeability in that context depends on three factors: contracts, technology, and actual or implied knowledge. Forum selection clauses found in website terms of use agreements or transactional click-wrap agreements allow parties to mutually determine an appropriate jurisdiction in advance of a dispute. They therefore provide important evidence as to the foreseeability of being hauled into the courts of a particular jurisdiction. Newly-emerging technologies that identify geographic location constitute the second factor. These technologies, which challenge widely held perceptions about the Internet's architecture, may allow website owners to target their content to specific jurisdictions or engage in 'jurisdictional avoidance' by 'de-targeting' certain jurisdictions. The third factor, actual or implied knowledge, is a catch-all that incorporates targeting knowledge gained through the geographic location of tort victims, offline order fulfilment, financial intermediary records, and web traffic.[65]

Trend of adopting a combination of Zippo 'Sliding Scale' and Calder 'Effects' test

The courts in the USA have recently adopted a combination of the *Zippo* 'sliding scale' test and the *Calder* 'effects' test in order to examine whether the forum court has jurisdiction in a case involving trademark infringement by the use of the internet.

In *Toys "R" US v. Step Two*,[66] the Court of Appeals revisited the issue. In that case, the plaintiff, Toys "R" Us (Toys), a Delaware corporation with its headquarters in New Jersey, owned retail stores worldwide where it sold toys, games, and numerous other products. In August 1999, Toys

[65] *Supra* note 9, at 1385.
[66] 318 F.3d 446 (3d Cir. 2003).

"R" Us acquired Imaginarium Toy Centers, Inc., which owned and operated a network of 'Imaginarium' stores for the sale of educational toys and games. In this process, Toys "R" Us also acquired several Imaginarium trademarks. The defendant, Step Two, was a corporation in Spain that owned or franchised toy stores operating under the name 'Imaginarium' in Spain and nine other countries. It had registered the Imaginarium mark in several countries where its stores were located. At the time of the litigation, there were 165 Step Two Imaginarium stores possessing the same unique facade and logo as the stores owned by Toys "R" Us, and selling the same types of merchandise as Toys "R" Us sold in its Imaginarium stores. However, Step Two did not operate any stores, maintain any offices or bank accounts, or have any employees anywhere in the United States. In 1995, Imaginarium Toy Centers, Inc. (which Toys "R" Us had later acquired) registered the domain name 'imaginarium.com' and launched a website featuring merchandise sold at Imaginarium stores. In 1996, Step Two registered the domain name 'imaginarium.es', and also began to advertise the merchandise that was available at its Imaginarium stores. In April 1999, Imaginarium Toy Centers registered the domain name 'imaginarium.net', and launched another website where it offered Imaginarium merchandise for sale. In June 1999, Step Two registered two domain names, 'imaginariumworld.com' and 'imaginarium-world.com'. In May 2000, Step Two also registered three more domain names including 'imaginariumnet.com' and 'imaginariumnet.org'. Toys "R" Us brought action against Step Two alleging that Step Two had used its websites to engage in trademark infringement, unfair competition, misuse of the trademark notice symbol, and unlawful 'cybersquatting.' The District Court of New Jersey denied Toys "R" Us' request for jurisdictional discovery and, simultaneously, granted Step Two's motion to dismiss for the lack of personal jurisdiction. However, the Court of Appeals held that the record did not support the finding that the defendant Step Two had knowingly conducted business with residents of New Jersey. It reversed and remanded the case for limited jurisdictional discovery relating to Step Two's business activities in the United States. The Court emphasized that:

> the mere operation of a commercially interactive website should not subject the operator to jurisdiction anywhere in the world. **Rather, there must be evidence that the defendant 'purposefully availed' itself of conducting activity in the forum state, by directly targeting its website to the state, knowingly interacting with residents of the forum state via its website, or through sufficient other related contacts**.[67] (Emphasis Supplied)

[67] *Id.* at 454.

The California Supreme Court in *Pavlovich v. Superior Court*[68] was divided 4:3 on the question of whether a Texas website operator who had posted software designed to defeat the plaintiff's technology for encrypting copyrighted motion pictures was subject to personal jurisdiction in California where the motion picture, computer, and DVD industries were centred. In rejecting jurisdiction, the majority focused on the fact that the defendant did not know that the particular plaintiff, a licensing entity created by the motion picture and DVD industries, was located there. The dissent thought it sufficient that the defendant was on notice that its conduct would harm the motion picture and DVD industries centred in California. In *Revell v. Lidov*,[69] the plaintiff, a Texas resident sued Lidov, a Massachusetts resident and the Columbia University for posting a defamatory piece on the university's bulletin board. The court applied both *Zippo* and *Calder*. It first found that the website was interactive and individuals could both send and receive messages. But applying *Calder* it found that the article made no reference to Revell's Texas activities and was not directed at Texas readers as distinguished from other readers. Also, Lidov did not know that Revell was a Texas resident when he posted the article and therefore could not reasonably anticipate being hauled into a Texas court. Consequently, the Texas court was held not to have jurisdiction.

Difficulties in the application of the three tests

Thomas Schultz points out that the dynamics of jurisdiction are reasonableness and fairness.[70] Schultz concludes that both the subjective territoriality and objective territoriality or the effects tests, if construed too broadly, are bound to be unfair and unreasonable. According to Schultz, a middle path had to be chosen between the too narrow ('subjective territoriality') and the too broad ('effects') jurisdictional bases for better managing transborder externalities. This middle path was 'targeting.' Schultz defines targeting to mean "in essence that the activity must be intended to have effects within the territory of the state asserting jurisdiction."[71] According to another scholar, Michael Geist, the principle of targeting is used to "identify the intentions of the parties and to assess the steps taken to either enter or avoid a particular jurisdiction."[72] Targeting is described as "something more than effects, but less than physical presence."[73]

---

[68] 58 P.3d 2 (Cal. 2002).
[69] 317 F.3d 467 (5th Cir. 2002).
[70] Thomas Schultz, *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, 19 EUR. J. INT'L L. 779 (2008).
[71] *Id.*
[72] *Supra* note 9, at 1357.
[73] *Supra* note 9, at 1357.

Legal scholars C. Douglas Floyd and Shima Baradaran-Robison add:

> Nor is the central difficulty in Internet cases created by the fact that a defendant has undertaken conduct that might subject itself to jurisdiction everywhere, rather than only in one or a few states. A tortfeasor who mails a thousand bombs to recipients in one state, and one to recipients in each of the other forty-nine states, should not be relieved from geographic responsibility for the consequences of his actions in each of those states simply because he is subject to suit everywhere, or because his conduct has a uniquely intensive relationship with a single state. The problem in Internet cases is not that the defendant is potentially subject to suit everywhere, but that he is potentially subject to suit anywhere, without having any particular reason to know where that might be. This lack of predictability and geographically specific notice lies at the heart of the difficulties that the courts have experienced in applying traditional jurisdictional concepts in cases in which the instrument of wrongdoing is an Internet posting. The case of the Internet posting is more analogous to one in which a defendant throws a bottle containing poisonous gas into the ocean, with awareness that it may cause injury to someone, somewhere, if it is found and opened someday.[74]

After discussing the inconsistent results arrived at by courts in different cases having more or less similar facts, they emphasise the need for a uniform approach, whether the cases involve torts, or inter-state commerce disputes. Thereafter they conclude:

> (1) A unified approach to questions of personal jurisdiction should be applied to all cases in which jurisdiction is asserted in a forum remote from the defendant's residence or the place of wrongdoing, regardless of the particular subject matter of the action, the legal theories that it raises, or the means by which the allegedly wrongful conduct of the defendant has been committed. (2) The factors informing such an approach must be sufficiently flexible to take account of the wide array of differing contexts in which issues of personal jurisdiction are presented, and, in particular, to take account of the unique characteristics of the Internet that have increasingly troubled the courts in recent years. (3) The Supreme Court's apparent importation of notions of a defendant's purpose or its intent to target the forum state is flawed and has created more problems than it has resolved in the context of modern actions involving informational torts. (4) Questions of personal jurisdiction should turn on objective (rather than subjective) factors that have primary reference to whether the defendant objectively should be on notice that it has caused the effects giving rise to the action in the particular forum state. If such notice does exist, the court should further inquire whether the intervening acts of third parties should relieve the defendant of geographic responsibility for those effects and

[74] C. Douglas Floyd & Shima Baradaran-Robison, *Toward a Unified Test of Personal Jurisdiction in an Era of Widely Diffused Wrongs: The Relevance of Purpose and Effects*, 81 IND. L.J. 602, 659 (2006).

> whether the balance of the interests of the defendant, the plaintiff, and the forum state makes it fundamentally unfair to subject the defendant to suit there.[75]

To summarise the position in the US, in order to establish the jurisdiction of the forum court, even when a long arm statute exists, the plaintiff would have to show that the defendant 'purposefully availed' of jurisdiction of the forum state by 'specifically targeting' customers within the forum state. A mere hosting of an interactive web page without any commercial activity being shown as having been conducted within the forum state, would not enable the forum court to assume jurisdiction. Even if one were to apply the 'effects' test, it would have to be shown that the defendant specifically directed its activities towards the forum state and intended to produce the injurious effects on the plaintiff within the forum state. Some courts have required the plaintiffs to show that the defendant should be shown to have foreseen being 'hauled' into the courts in the forum state by the very fact that it hosted an interactive website.

OTHER COMMON LAW JURISDICTIONS

The approach of courts in other common law jurisdictions, including India, is examined next.

Canada

In *Morguard Investments Ltd. v. De Savoye*,[76] the Canadian Supreme Court emphasized the 'real and substantial connection' as a test for determining jurisdiction. It was observed that the approach of permitting suit where there is a real and substantial connection with the action strikes an appropriate and reasonable balance between the rights of the parties. In *Pro-C Ltd. v. Computer City Inc.*,[77] it was held that the listing of Canadian retail outlets on the defendant's website coupled with there being a *de-facto* 'common market' between Canada and the US meant that Canadian consumers were being targeted and therefore the Ontario court in Canada would have jurisdiction to try the trademark infringement action against the defendant located in the USA.

In *Patrick Desjean v. Intermix Media Inc.*,[78] the defendant, a Delaware Corporation with its principal office in Los Angeles, used to offer ostensible free software programs. When the plaintiff, a resident of Canada, installed a free Intermix Screensaver or game from www.mycoolscreen.com, he also unwittingly installed one or more spyware programs. Thereafter, the plaintiff brought an

---

[75] *Id.* at 604-605.
[76] [1990] 3 S.C.R. 1077 (Can.).
[77] 7 C.P.R. (4th) 193 (Can.), *rev'd*, 205 D.L.R. (4th) 568 (Can.).
[78] 2006 F.C. 1395 (Can.).

action against the defendant in Canada for violating the misleading representations provisions of the Canadian Competition Act, 1985. The Federal Court of Ottawa, after referring to the decision of the Ontario Court of Appeal in *Muscutt v. Courcelles*, (2002) 213 D.L.R. (4th) 577, took the following eight factors into account while determining whether it had jurisdiction:

> (1) The connection between the forum and the plaintiff's claim; (2) The connection between the forum and the defendant; (3) Unfairness to the defendant in assuming jurisdiction; (4) Unfairness to the plaintiff in not assuming jurisdiction; (5) Involvement of other parties to the suit; (6) **The Court's willingness to recognize and enforce an extra-provincial judgment rendered on the same jurisdictional basis**; (7) Whether the case is interprovincial or international in nature; (8) **Comity and standards of jurisdiction, recognition and enforcement prevailing elsewhere**.[79] (Emphasis Supplied)

The Court observed that the defendant had no office in Canada although in the past it subsidized office space for contractors working on two websites purchased by Intermix. Intermix had no server in Canada and www.mycoolscreen.com also was not hosted on servers located in Canada but on a server in California. It was also observed that 66% of downloads from either the defendant's websites or third parties distributing the defendant's applications were made by American users and the remaining were made throughout the world. Canada accounted for only 2.5% to 5.3% of downloads. On the basis of these facts, the Federal Court held that the Canadian courts had no jurisdiction over the defendant since there was no substantial connection between the defendant and the forum. What is significant is that the Canadian federal Court identified the court's willingness to recognise and enforce an extra-provincial judgement rendered on the same jurisdictional basis as being a relevant factor. It highlights the need for reciprocity and its relevance in enforcement without which exercise of such personal jurisdiction over extra-territorial defendants might be rendered futile.

United Kingdom

In *1-800 Flowers Inc. v. Phonenames*,[80] the defendant was a UK based phonebook company and the plaintiff was engaged in the business of delivery of flowers. Customers across the world could access the plaintiff's website to place orders for flowers. There was, however, no evidence to show that UK residents had placed orders on its website. It was argued that because the website was accessible from the UK and the UK residents could place orders online, the use by the defendant

[79] *Id.* at ¶ 27.
[80] [2002] F.S.R. 12 (C.A.) (U.K.).

of the mark 1-800 on its website amounted to use in the UK. It was held in the first appeal by the Bench that "mere fact that websites could be accessed anywhere in the world did not mean, for trade mark purposes, that the law should regard them as being used everywhere in the world."[81] The intention of the website owner and what the reader will understand if he accesses the website was held to be relevant. The Court of Appeals also rejected the argument. Justice Buxton, in a concurring opinion pointed out as under:

> I would wish to approach these arguments, and particularly the last of them, with caution. There is something inherently unrealistic in saying that A 'uses' his mark in the United Kingdom when all that he does is to place the mark on the internet, from a location outside the United Kingdom, and simply wait in the hope that someone from the United Kingdom will download it and thereby create use on the part of A. By contrast, I can see that it might be more easily arguable that if A places on the internet a mark that is confusingly similar to a mark protected in another jurisdiction, he may do so at his peril that someone from that other jurisdiction may download it; though that approach conjured up in argument before us the potentially disturbing prospect that a shop in Arizona or Brazil that happens to bear the same name as a trademarked store in England or Australia will have to act with caution in answering telephone calls from those latter jurisdictions. However that may be, the very idea of 'use' within a certain area would seem to require some active step in that area on the part of the user that goes beyond providing facilities that enable others to bring the mark into the area. Of course, if persons in the United Kingdom seek the mark on the internet in response to direct encouragement or advertisement by the owner of the mark, the position may be different; but in such a case the advertisement or encouragement in itself is likely to suffice to establish the necessary use.[82]

Australia

The judgment of the Australian High Court in *Dow Jones & Company Inc. v. Gutnick*,[83] is instructive of the application of the effects test. Dow Jones & Company Inc., a corporation registered in the USA, had published material on the internet that was allegedly defamatory of Mr. Gutnick who sued in the Supreme Court of Victoria to recover damages to vindicate his reputation. The Victorian law was treated as a long arm rule which provided for jurisdiction based upon the mere happening of damage within a jurisdiction. The High Court held that the primary judge was correct in deciding the issue of jurisdiction in favour of the plaintiff. Since the long arm was found to be valid and applicable, the arguments that the defendant had minimal commercial interest in

[81] *Id.*
[82] *Supra* note 80.
[83] (2002) H.C.A. 56 (Austl.).

the sale of its magazine in Victoria and that it had published them principally for the benefit of US readers was considered irrelevant. However, what is important to note is that the state of Victoria in the said case did have a long arm law which was held to be valid and which permitted extension of jurisdiction.

India

Casio India Co. Limited v. Ashita Tele Systems Pvt. Limited[84] was a passing off action where the defendant was carrying on business from Bombay. The defendant had managed to get a registration of domain name www.casioindia.com and defendant no. 2 was the Registrar with whom the domain name had been registered. The plaintiff, on the other hand, claimed to be a 100% subsidiary of Casio Computer Ltd., Japan (Casio Japan), which was the registered owner of the trade mark 'Casio' in India used for a large number of electronic and other products. He had registered a large number of domain names in India like 'CasioIndiaCompany.com', 'CasioIndia.org', 'CasioIndia.net', etc. Defendant No. 1 had obtained the above domain names during the time when it held a distributorship agreement with the plaintiff. It was held by the learned single Judge after referring to the decisions in *Rediff Communication Ltd. v. Cyber Booth*[85] and *Dow Jones & Co. Inc. v. Gutnick*[86] that "once access to the impugned domain name website could be had from anywhere else, the jurisdiction in such matters cannot be confined to the territorial limits of the residence of the defendant."[87] According to the learned single Judge, since a mere likelihood of deception, whereby an average person is likely to be deceived or confused was sufficient to entertain an action for passing off, it was not at all required to be proved that "any actual deception took place at Delhi. Accordingly, the fact that the website of Defendant No. 1 can be accessed from Delhi is sufficient to invoke the territorial jurisdiction of this Court."[88]

In *India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc & Ors.*,[89] a different approach was adopted. The plaintiff ran a Hindi news channel 'INDIA TV' that was launched in March 2004. However, the plaintiff claimed to have adopted the trademark 'INDIA TV' since December 2002. The plaintiff had applied for registration of the said mark and the relevant

---

[84] 2003 (27) P.T.C. 265 (Del.) (India), *overruled by* Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy, CS(OS) 894/2008 (High Court of Delhi, 23rd November 2009) (India).
[85] A.I.R. 2000 Bom. 27 (India).
[86] *Supra* note 83.
[87] *Supra* note 84, at ¶ 6.
[88] *Supra* note 84, at ¶ 6.
[89] 2007 (35) P.T.C. 177 (Del.) (India).

applications had been published in the trademarks journal. The plaintiff was also the owner of the domain name 'indiatv.com' which was registered on 18.11.2003. The channel was made available for live viewing on the said website. Defendant Nos. 1 & 2 hosted a website 'www.indiatvlive.com' which the plaintiff came across in January 2007. The website contained the words 'INDIA TV' which were displayed prominently inside the sketch of a television. A passing off action was initiated in the Delhi High Court to prevent Defendant No. 2 from using the domain name 'www.indiatvlive.com.' While the suit was pending, Defendant No. 1 was proceeding with an action instituted by it in the Arizona District Court in USA, where the defendants were located, against the plaintiff seeking a declaration of non-infringement of the plaintiff's mark by Defendant No. 1. The plaintiff then approached the Delhi High Court stating that the defendant had suppressed the fact of having filed the aforesaid action in Arizona and prayed for an injunction against defendant from proceeding with the said action in the Arizona courts particularly since the suit in the Delhi High Court was a prior action. In resisting the said application, Defendant No. 1 took the stand that the Delhi High Court was not a court of competent jurisdiction as it was not the appropriate forum/*forum conveniens*. Inasmuch as the defendants did not reside or work for gain in India, it was only the District Court in Arizona that was the appropriate forum/*forum conveniens* to decide the dispute. It was argued before the court that in order to attain personal jurisdiction, i.e., jurisdiction over the person of a defendant in contrast to the jurisdiction of a court over a defendant's property or his interest therein, there should be a long arm statute on the basis of which the court could exercise jurisdiction over any individual located outside the state. As regards the internet, it was argued that it was not enough to establish that there was a passive website. The court referred to the purposeful availment test and the three factors highlighted in *Cybersell*. The learned single Judge then noticed that India did not have a long arm statute to grant jurisdiction as regards non-resident defendants. Therefore it had to be examined whether the defendant's activities "have a sufficient connection with the forum state (India); whether the cause of action arises out of the defendant's activities within the forum and whether the exercise of jurisdiction would be reasonable." In paragraphs 46 and 47, it was observed as under:

> 46. I am in agreement with the proposition that the mere fact that a website is accessible in a particular place may not itself be sufficient for the courts of that place to exercise personal jurisdiction over the owners of the website. However, where the website is not merely 'passive' but is interactive permitting the browsers to not only access the contents thereof but also subscribe to the services provided by the owners/operators, the position would be different. However, as noticed in the judgment in CyberSell Inc. case (supra), even where a website is interactive, the level of interactivity would be relevant and limited interactivity may also not be sufficient for a court to exercise jurisdiction. In Panavision International LP case

> (supra), it was found that the registration of the Plaintiff's mark as a domain name by the Defendant had the effect of injuring the Plaintiff in California and therefore the court had jurisdiction. In Compuserve case (supra) again it was found that the Defendant had contacted Ohio to sell his computer software's on the Plaintiff's Ohio based systems and sent his goods to Ohio further for their ultimate sale and thus those courts had jurisdiction.
> 47. In the present case, the website 'indiatvlive.com' of Defendant No. 1 is not wholly of a 'passive' character. It has a specific section for subscription to its services and the options (provided on the website itself) for the countries whose residents can subscribe to the services include India. The services provided by Defendant No. 1 can thus be subscribed to and availed of in Delhi (India) i.e. within the jurisdiction of this court.[90]

The learned Single Judge concluded in *India TV* that "Defendant No. 1 intended to target expatriate Indians as well as Indians within the country."[91] Furthermore, the stand taken by Defendant No. 1 in its written statement was that it had a global presence including a presence in India. It claimed to be the first IPTV delivery system for Indian content from India. The website of Defendant No. 1 was launched in India as well as in Los Angeles. It was accordingly held that "Defendant No. 1 company has sufficient connection with India."[92] As regards the 'effects' test, it was held that since the plaintiff channel was an Indian news channel intended for Indian audiences, any damage alleged to have been caused or alleged to be likely to arise to the good will, reputation, etc. of the plaintiff would be in India. However, the alleged damage that may have arisen or may be likely to arise to the plaintiff would be as a consequence of the fact that the impugned website is accessible in India and the services provided can be availed of in India. Consequently, it was held that "the Defendant is carrying on activities within the jurisdiction of this court; has sufficient contacts with the jurisdiction of the court and the claim of the Plaintiff has arisen as a consequence of the activities of Defendant No. 1 within the jurisdiction of this court."[93]

Both *Casio* and *India TV* were decisions of single Judges and required proper reconciliation. The opportunity presented itself in *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*.[94] The

---

[90] *Id.* at ¶ 46-47.
[91] *Supra* note 89, at ¶ 49.
[92] *Supra* note 89, at ¶ 49.
[93] *Supra* note 89, at ¶ 51.
[94] CS(OS) 894/2008 (High Court of Delhi, 23rd November 2009) (India).

plaintiff there was a company located in Singapore. It claimed that it was part of a group of companies involved in the hospitality business. It claimed the use of the word mark 'Banyan Tree' and also the banyan tree device since 1994. The plaintiff maintained the websites 'www.banyantree.com' and 'www.banyantreespa.com' since 1996. The websites were accessible in India. Its application for the registration of the mark and the device were also pending. In October 2007, the plaintiff learnt that the defendants, located in Hyderabad in Andhra Pradesh, had initiated work on a project under the name 'Banyan Tree Retreat', which according to the plaintiff was deceptively similar to that of the plaintiff. The plaintiff invoked the jurisdiction of the Delhi High Court on the ground that the defendants' website 'www.makprojects.com/banyantree', which advertised its products and services was accessible in Delhi. The display of the confusingly similar mark and device was calculated to cause much confusion and deception among the public by passing off the services of the defendants as that of the plaintiff. Accordingly, an injunction was sought. The Division Bench of the Delhi High Court, while answering the referral order of the learned Single Judge, affirmed the ruling in *India TV* and overruled *Casio*. It then remanded the case to the single Judge for a decision on the preliminary issue of jurisdiction.

The answers given by the Division Bench in *Banyan Tree* to the questions of law referred to it were as follows:

> Question (i): For the purposes of a passing off action, or an infringement action where the plaintiff is not carrying on business within the jurisdiction of a court, in what circumstances can it be said that the hosting of a universally accessible website by the defendants lends jurisdiction to such Court where such suit is filed ('the forum court')?
>
> Answer: For the purposes of a passing off action, or an infringement action where the plaintiff is not carrying on business within the jurisdiction of a court, and in the absence of a long-arm statute, in order to satisfy the forum court that it has jurisdiction to entertain the suit, the plaintiff would have to show that the defendant 'purposefully availed' itself of the jurisdiction of the forum court. For this it would have to be prima facie shown that the nature of the activity indulged in by the defendant by the use of the website was with an intention to conclude a commercial transaction with the website user and that the **specific targeting** of the forum state by the defendant resulted in an injury or harm to the plaintiff within the forum state.
>
> Question (ii): In a passing off or infringement action, where the defendant is sought to be sued on the basis that its website is accessible in the forum state, what is the extent of the burden on the plaintiff to prima facie establish that the forum

> court has jurisdiction to entertain the suit?
>
> Answer: For the purposes of Section 20(c) CPC, in order to show that some part of the cause of action has arisen in the forum state by the use of the internet by the defendant the plaintiff will have to show prima facie that the said website, whether euphemistically termed as 'passive plus' or 'interactive', was specifically targeted at viewers in the forum state for commercial transactions. The plaintiff would have to plead this and produce material to prima facie show that some commercial transaction using the website was entered into by the defendant with a user of its website within the forum state resulting in an injury or harm to the plaintiff within the forum state.[95] (Emphasis Supplied)

It was held that merely having an interactive website was not sufficient to make the defendant amenable to the jurisdiction of the forum court. Applying the principle of intentional targeting, it was held that the plaintiff had to show the intention of the defendant to conclude a commercial transaction with the website user.

Banyan Tree also dealt with the issue of trap orders. The question that was addressed was whether a single trap transaction was sufficient to show that the defendant had purposefully availed the forum Court's jurisdiction. It was held that a lone trap transaction will not be sufficient evidence for the purposes of establishing that a part of the cause of action arose within the jurisdiction of the court. The plaintiff would have to show that the defendant has purposefully availed of the jurisdiction of the forum court by entering into a commercial transaction with an internet user located within the jurisdiction of the forum court. This cannot possibly result from a solitary trap transaction since that would not be an instance of 'purposeful' availment by the defendant. It would have to be a real commercial transaction that the defendant has with someone and not a transaction set up by the plaintiff itself. If the only evidence is in the form of a series of trap transactions, they have to be shown to be obtained using fair means. The plaintiff seeking to establish jurisdiction on the basis of such trap transactions would have to aver unambiguously in the plaint, and also place along with it supporting material that prima facie proves that the trap transactions relied upon satisfy the above-mentioned test.

---

[95] *Id.* at ¶ 59.

Banyan Tree has been later followed by the Karnataka High Court in *Presteege Property Developers v. Prestige Estates Projects Pvt. Ltd.*,[96] a case involving a passing off action initiated by Prestige Estates against Presteege Property Developers. The Single Judge noticed that the construction activity of the defendant[97] was exclusively in Kerala. It was further observed that though online booking was indicated, the sale would not take place in Bangalore so as to constitute a part of the cause of action in terms of passing off since even if the defendants were to pass off their property riding on the reputation of the plaintiff as alleged, the same would take place only in Kerala. Similarly in the case of the other defendant,[98] the activity of providing the services was observed to be exclusively in Tamil Nadu. The court held that the "test of concluding a commercial transaction should be shown, to establish the level of activity indulged in by the defendants by the use of the website."[99] The test not being satisfied by the plaintiff,[100] the learned single Judge held that the court at Bangalore would lack jurisdiction.

The present state of the law in India may be summarized. A plaintiff, not having the benefit of the limited long arm provision of either section 134 of the Trade Marks Act, 1999 or section 62 of the Copyright Act, 1957 will not be able to persuade a court to exercise jurisdiction over a defendant hosting a website containing the material purportedly violating the plaintiff's IP rights unless it is shown that the defendant targeted its interactive website at viewers in the forum state for the purpose of commercial transactions and in fact entered into such transactions using the website. Further a lone trap transaction may not demonstrate the 'purposeful' targeting by the defendant of the forum state or of 'aiming' at particular customers therein. A more systematic behaviour over a series of transactions will have to be shown as having been entered into by the defendant. It may be argued that the test evolved in *Banyan Tree* may not answer the problems in a different factual setting and in a different context, for e.g., the tort of defamation or the crime of cyber pornography. But then *Banyan Tree* does not deal with those contexts for which other tests will have to be devised. Nevertheless the courts in India will have to guard against over-protection of local interests and adopt a balanced approach to ensure that a middle path is found in individual cases.

---

[96] MFA 4954 & 13696/2006 (High Court of Karnataka, 2nd December 2009) (India); *see also* Sholay Media Entertainment & Anr. v. Yogesh Patel & Ors. CS(OS) 1714/2001 (High Court of Delhi, 27th January 2010) (India).
[97] MFA 4954/2006 (High Court of Karnataka, 2nd December 2009) (India).
[98] MFA 13696/2006 (High Court of Karnataka, 2nd December 2009) (India).
[99] *Id.*
[100] Respondent in MFA 4954 & 13696/2006 (High Court of Karnataka, 2nd December 2009) (India).

III

OTHER TYPES OF CASES

Internet Jurisdiction in Copyright Cases

The tests adopted in copyright cases for exercising jurisdiction are no different from those already discussed. The courts in the USA that had earlier sought to fashion constitutional tests for jurisdiction around the particular technologies of the internet, have in the more recent decisions reverted to the known tests of minimum contacts and reasonableness.

ALS Scan, Inc. v. Digital Service Consultants, Inc.[101] is an example of the contemporary trend. The defendant, a Georgia-based Internet service provider, argued that it conducted no business and had no offices, contracts, income, or advertising (other than through its website) in Maryland. The plaintiff, a Maryland corporation, countered that, by enabling a third-party website operator to publish allegedly infringing photographs in Maryland, the defendant had subjected itself to specific jurisdiction in the state. The court ruled for the defendant, observing that:

> [i]f we were to conclude as a general principle that a person's act of placing information on the Internet subjects that person to personal jurisdiction in each State in which the information is accessed, then the defence of personal jurisdiction, in the sense that a State has geographically limited judicial power, would no longer exist.[102]

The court formulated a general rule that would establish personal jurisdiction in at least some of these cases:

> a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts.[103]

The court added, however, that under such a standard, a person who simply places information on the internet does not subject himself to jurisdiction in each state into which the electronic signal is

---

[101] 293 F.3d 707 (4th Cir. 2002).
[102] *Id.* at 712.
[103] *Supra* note 95, at 714.

transmitted and received. This decision is also an instance of the exemption of an ISP from liability merely because it provided a platform or space in which the alleged infringement took place.[104]

In *Bridgeport Music, Inc v. Still N the Water Publishing*,[105] it was recognized that just operating an internet website can constitute purposeful availment if the website is interactive to a degree that entails specifically intended interaction with state residents. The court held that there was no jurisdiction in Tennessee over a defendant that had not hosted or operated a website for sale of alleged infringing composition.

Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.[106] involved the free exchange of copyrighted music, movies and other digital media over the internet. The defendants distributed software that enabled users to exchange digital media via the same peer-to-peer transfer network. When the actions were originally filed, the defendants (Grokster, MusicCity and Kazaa BV) each independently branded, marketed and distributed file-sharing software. All three platforms were powered, however, by the same 'FastTrack' networking technology. This technology was developed by defendants Niklas Zennstrom and Janus Friis (who also launched Kazaa BV), and licensed to each company. As a result, users of all three software platforms were connected to the same peer-to-peer 'FastTrack network,' and were able to exchange files seamlessly. However, later the operation of the 'Kazaa system' had passed from Kazaa BV to Sharman Networks, a company organized under the laws of the island-nation of Vanuatu and doing business principally in Australia. The defendant had allegedly provided file-sharing software and entered into licensing agreements with approximately two million Californian residents. The Court explained that in order to extend personal jurisdiction, it would have to be shown that (1) a non-resident defendant purposefully availed itself of the privilege of conducting activities in the forum state, thereby invoking the protections of its laws; and (2) the plaintiff's claims arose out of the defendants' forum-related activities. In the instant case, it was held that the defendant was subject to specific jurisdiction under the California long arm statute because it directed its commercial activities at California, the forum state, and alternatively because of the impact of the defendant's activities in California. While determining that the defendant

[104] The position in India as regards liability of intermediaries is that an intermediary is exempt from liability under certain conditions as per the Information Technology Act, 2000, No. 21 of 2000 ('IT Act'), as amended further by the Information Technology (Amendment) Act, 2008, No. 10 of 2009. The definition of an 'intermediary' under section 2(w) of the Act has also undergone a change. The Amendment Act of 2008 has further substituted the older section 79 with a new one, which now more elaborately deals with exemption of intermediaries.

[105] 327 F.3d 472, 483 (6th Cir. 2003).

[106] 243 F. Supp. 2d 1073 (C.D. Cal. 2003).

had engaged in commercial activities directed at the forum State, the *Grokster* court cited *Cybersell* and *Zippo*. For the effects test, the *Grokster* court drew on the Supreme Court's decision in *Calder*.

IV

ENFORCEMENT

The territorial nature of IPR is challenged by the advent of the internet. Attempts at finding a uniform minimum standard to decide issues of jurisdiction as well as applicable law are still to bear any definite shape. The TRIPS framework fails to provide the necessary platform for resolving trans-border disputes arising out of the use of the internet. In the circumstances, reliance is increasingly placed on the available enforcement mechanisms in private international law to protect IPRs in digital goods distributed on web-based networks.

Courts in domestic jurisdictions rely upon long arm statutes that enable them to exercise personal jurisdiction over defendants outside the territory of the forum state. In some of the cases noticed hereinbefore, particularly from the courts in the USA, the readiness with which jurisdiction has been exercised is explained with reference to the existence of long arm statutes in some of the States. In India, in the absence of a federal structure (as in the USA) in that sense, the provision enabling the Courts to exercise jurisdiction with such a 'long arm' is present in section 20 (c) of the Code of Civil Procedure, 1908 (CPC) that confers jurisdiction to courts wherever there is an accrual of any "cause of action, wholly or in part." For trademark infringement suits or suits relating to any right in a "registered trademark", Section 134(2) of the Trade Marks Act, 1999 supplements the courts to exercise jurisdiction over a non-resident defendant, where the plaintiff "actually and voluntarily resides or carries on business or personally works for gain." A similar provision to that effect is present in section 62 of the Copyright Act, 1957 for suits filed against copyright infringement.

However, exercising jurisdiction is only one part of the exercise. The forum court's intervention would be rendered futile if its orders against defendants outside its jurisdiction cannot be enforced. This is compounded if the defendant has no assets within the forum state. Further, where the defendant is protected by the laws of his country against the consequence brought about the judgment, the courts in the country of the defendant would be reluctant to accord recognition and consequent enforcement of such judgment.

The case of *Yahoo! Inc. v. LICRA*[107] is illustrative of such complex legal situations. Yahoo!, an American internet service provider, brought suit in federal district court in diversity against La Ligue Contre Le Racisme et L'Antisemitisme ('LICRA') and L'Union des Etudiants Juifs de France ('UEJF') seeking a declaratory judgment that two interim orders by a French court are unrecognizable and unenforceable. The district court held that the exercise of personal jurisdiction over LICRA and UEJF was proper, that the dispute was ripe, that abstention was unnecessary, and that the French orders are not enforceable in the United States because such enforcement would violate the First Amendment. The district court did not reach the question whether the orders are recognizable. LICRA and UEJF appealed only the personal jurisdiction, ripeness, and abstention holdings. A majority of the en banc panel (Court of Appeals) held that the district court properly exercised personal jurisdiction over LICRA and UEJF. The Court of Appeals reversed the District Court. While three judges alone held that the District Court did not have jurisdiction over the French defendants and therefore the suit should be dismissed, three other judges held that the suit was not ripe and therefore, should be dismissed. Consequently, by a 6:5 majority, the suit was dismissed.

The relevant passage clarifying the opinion of the Court of Appeal is given below:

> An eight-judge majority of the en banc panel holds, as explained in Part II of this opinion, that the district court properly exercised specific personal jurisdiction over defendants LICRA and UEJF under the criteria of Calder. A three-judge plurality of the panel concludes, as explained in Part III of this opinion, that the suit is unripe for decision under the criteria of Abbott Laboratories. When the votes of the three judges who conclude that the suit is unripe are combined with the votes of the three dissenting judges who conclude that there is no personal jurisdiction over LICRA and UEJF, there are six votes to dismiss Yahoo!'s suit.[108]

In the Indian context, as long as the disputes concern parties that are within the country, the question of enforcement of the judgment of one state court in another state where the defendant resides or carries on business may not arise in view of the provisions of the Civil Procedure Code. However, where the defendant is outside the country, unless there are reciprocal arrangements for recognition of decrees entered into the country of the defendant's location, enforcement will be problematic. Further, in the context of the internet, the web server hosting the offending material will have to abide by the order of the court asking it to remove the offending material from the

[107] Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme, 433 F.3d 1199 (9th Cir. 2006).
[108] *Id.* at 1124.

website or block the site from viewership. Although this is technically feasible, it would not be legally achievable unless the entity required to implement the court's directions accepts and agrees to abide by them.

Wendy Adams brings out the complex nature of the problem in the following passage:

> When differences in the extent to which states assume jurisdiction over disputes involving extraterritorial activity are combined with the jurisdictional ambiguity inherent in an on-line environment, unilateral enforcement of intellectual property rights within virtual commerce is not a viable alternative; domestic adjudication cannot reconcile protection ahead of the curve with the minimum standards provided under the terms of the TRIPS Agreement in a manner which preserves but does not enhance TRIPS entitlements. In ensuring the legitimacy of private enforcement, the methodology adopted to map virtual transactions to territorial jurisdiction is a critical factor. Deficiencies in the localization process would permit infringement in violation of domestic law, resulting in undercompensation of domestic innovators relative to foreign imitators. In the alternative, domestic courts could also settle problems of jurisdictional ambiguity by stretching the notion of territoriality beyond currently accepted limits. Excessive localization would amount to an impermissible extraterritorial application of domestic intellectual property law, leading to overcompensation of local innovators. Foreign imitators would be faced with a forced march to the top, particularly in relation to states possessing superior economic advantages in terms of trading power and as a desirable location for foreign direct investment.[109]

It is therefore not unusual that Alternative Dispute Resolution mechanisms through multilateral trade negotiations have been thought of. One such instance is the Uniform Domain Name Dispute Resolution Policy (UDRP) developed in the context of registration of domain names. To tackle the growing phenomenon of cyber squatting, the UDRP was brought forth by the ICANN. It provides a remedy by way of arbitration. It appears that the World Intellectual Property Organization ('WIPO') also has an Arbitration & Mediation Centre which adjudicates on disputes brought before it concerning the domain name registration. The Centre has been approached by prominent individuals and companies seeking permanent injunction against parties who registered domains in the names of such plaintiffs.

---

[109] *Supra* note 3.

A recent instance of invoking the jurisdiction of a court in India to prevent the name of a public figure being registered as a domain name, which can then be commercially sold on the website is *Arun Jaitley v. Network Solutions Private Limited & Ors.*[110] Mr. Jaitley, a prominent senior lawyer and politician, decided to book the domain www.arunjaitley.com through the website of the defendant nos. 1 and 2 (Network Solutions LLC) since defendant No.2 was the registering authority which had registered the domain name at the instance of some other person whose identity is not yet known. A WHOIS search conducted on the said domain name showed that on 21st July 2009 the Registrar for the domain name was defendant no.1 Network Solutions, LLC. It was found that the domain name had expired on 12th July 2009 and was pending deletion. Despite Mr. Jaitley's lawyer asking that no domain name be registered or renewed using his name, the defendants declined to do so. On 27th August 2009 when a search was conducted on WHOIS Search, the status of the domain name was continued to be shown as 'pending delete.' It had been updated on 21st August 2009. The Registrar for the said domain name was still shown as Network Solutions, LLC. On 31st August 2009 when a further WHOIS Search was conducted, it showed that the Registrar for the said domain name had changed to 'DOMAIN PARK BLOCK.COM LLC.' The Registrant was Portfolio Brains LLC (PBL) an entity which has been impleaded as Defendant No.3. In an interim order, the Delhi High Court observed:

> 25. The present suit raises very significant questions in the realm of intellectual property law concerning the protection that a person is entitled to, particularly when the person's name had acquired distinctiveness, goodwill and reputation. It also raises an important question whether the right to one's own name is part of the bundle of 'personal' rights enshrined in the right to life under the Article 21 of the Constitution of India, and Article 17 of the International Covenant on Civil & Political Rights. Is a person entitled to protection of such a right and all other rights incidental to and stemming from that right viz., the rights to publicity and to privacy. It appears to this Court that the plaintiff has more than a stateable prima facie case.
>
> 26. The plaintiff has prima facie demonstrated, with the help of all several documents, that defendant No.3 is 'squatting' on his name with the intention of exploiting it for profit. If not injuncted, the domain name www.arunjaitley.com could well be 'purchased' by any person. Such person could then use it for any purpose detrimental to the goodwill and reputation of the plaintiff. The balance of convenience in restraining the defendants from transferring, alienating or offering for sale the domain name 'arunjaitley.com' to any third party and from creating any third party interest in the said domain name 'arunjaitley.com' appears to be in favour of the plaintiff at this stage.[111]

[110] CS(OS) 1745/2009 (High Court of Delhi, 15th September 2009) (India).
[111] *Id.*

The court restrained PBL from advertising the domain name 'arunjaitley.com' or using the said domain name for auction purposes or for any other purpose. PBL was restrained from transferring, alienating or offering for sale the said domain name to any third party and from creating any third party interest in the said domain name and was directed to maintain status quo in relation to the said domain name. In other cases where offending emails are sought to be blocked, the court issues a mandatory injunction to the email service provider to ensure compliance with the court's directions. Problems could arise if those entities which are located outside the jurisdiction either refuse to answer summons or refuse to implement the court's directions. In that event, resort to the UDRP might be a more efficacious option for a plaintiff.

It appears that attempts at evolving a uniform law to govern the issue of enforceability of foreign judgments, with particular reference to disputes arising out of internet transactions proved unsuccessful. It appears that the Hague Convention on Choice of Court Agreements on June 30, 2005, does not cover the question of torts committed on the internet. The first draft of the Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters adopted in 1999 did not deal with issues arising from e-commerce and this was referred to a group of experts. They could not agree on any minimum uniform standard in view of the uncertain domestic law in the area.[112] This therefore is an unfinished task that will require to be revisited since the need for such a uniform law, given the volumes of transactions on the net, can never be overstated.

V

THE IMPORT OF JURISDICTIONAL ISSUES CONCERNING THE INTERNET

The above discussion throws up several interesting questions. One is whether the entire cyber world is in fact getting fragmented in the process of devising laws and procedures reflective of the tension between being overly protective of domestic interests and having too little regulation of the internet.

Wendy Adams contextualizes the pros and cons of 'universal permission' as opposed to 'universal prohibition' in the following words:

> Resolution of the issue of jurisdiction in relation to commercial websites that do not appear to be directed towards a specific territorial market requires that a default legal rule be established in favour of either the location of the commercial website

[112] *See* Holger Hestermeyer, *Personal Jurisdiction for Internet Torts: Towards an International Solution?*, 26 NW. J. INT'L L. & BUS. 267 (2006).

> (which may refer either to the location of the initial server, the location of one or more caching servers, or the website operator's usual place of business), or the location of the person accessing the website (an inquiry which could also be complicated by issues of nationality and residence). A default rule favouring the location of the website would amount to universal permission, whereby the commercial website operator is presumed to be in compliance with local regulation to which he is subject, and individual states must in effect opt-out of this rule by applying indirect regulation to prohibit residents from accessing commercial websites in violation of local laws. In contrast, a default rule favouring the location of the person accessing the commercial website would amount to universal prohibition; commercial website providers would be required to determine in advance those states in which their products are permitted, and allow residents of these states alone to opt-in by restricting access to the website accordingly. Note that these default rules are mutually-exclusive, and accordingly states must reach consensus in favour of permission or prohibition if consistent results are to be reached. Note as well that conditioning access upon geographical location becomes more complicated as successively smaller jurisdictional units are adopted, e.g., sub-state entities within federal unions and municipalities. Compelling arguments can be marshalled in support of either position, but what is immediately apparent is that a default rule of universal prohibition tends to reduce the efficacy of the Internet as a unique commercial medium, leading to what some commentators have called a Balkanisation of the Internet.[113]

Thomas Schultz is another legal scholar who has reflected on the above problem. He challenges in a direct way popular assumptions about the internet. The first assumption was that the internet was 'free' as in free speech. Schultz says, and rightly, that technology has demonstrated that it can be shaped 'so as to enshrine values of liberty or values of control.' He says: "It had been shown that the Internet could be a place of exquisite control just as it used to be a place of exquisite liberty. Thus, the first 'inherent characteristic' claim had been repealed."[114]

The other myth he seeks to demolish is that the internet is 'global'; that it was a large network of computers which had no centre or central authority through which all communications would travel and which could regulate those communications. It was conceived as an 'internet cloud' symbolising the unpredictability of the path that the communication could take from one point to another. However when governments the world over realized that the internet was just another

[113] *Supra* note 3.
[114] *Supra* note 70.

tool that could be misused for a variety of nefarious activities, they clamped down on the 'freedom' of access to the net.

> People started to say that they did not want outlandish foreigners to do the equivalent of standing in the garden in front of their house doing things that are regarded with outright repugnance in their community. The French were anxious at the thought of there being, just around the corner, defiant Americans believing it is their fundamental right to say whatever they want to say, even if it involves an apology for Nazism. In the United States, people were incensed about lax foreign governments not cracking down on online casinos, which were intruding into American homes and offices, computers, and mobile phones, to fuel compulsive gambling. Many countries became concerned about incitements to terrorism and appeals to fund terrorist organizations flowing into their country simply by dint of being globally accessible. Some governments began to consider blocking by technical means local residents' access to foreign Internet sources that glorify terrorism. Other governments grew increasingly apprehensive about the West spreading its culture and values throughout the world by a mere information transfer into territories which were previously exposed mainly to local information. Suddenly, the free and global character of the Internet started to be considered an evil. The global Internet community started to think that, after all, it did not want to be a single community, but several, and that each community should be allowed to live according to its internal fundamental values, according to its own choices of public policy (in the sense of ordre public), which partake of the expression of each nation's Volksgeist. The Internet should be free, most agreed, but only insofar as this freedom stopped short of violating the fundamental principles underlying the operation of each state's legal system.[115]

In the field of e-commerce, Schultz says, the re-emergence of the Westphalian outlook of states to protect 'local' values and their own 'sovereignty' is leading to fragmentation of the internet. He observes:

> The Internet is caught between old forces of local territorialism and new forces characteristic of global economies. As a result, it may end up being carved up or fragmented into discrete legal spheres - a development which contradicts the hitherto traditional vision of the Internet as a paradigmatic example of a borderless world of global transnationalism.
>
> The fragmentation is taking **two forms**. The first may be represented as **vertical** in nature; led by the forces of territorialism, it reflects concerns of public policy and

[115] *Supra* note 70.

> the protection of local values. The second, which may be considered **horizontal**, is driven by the rationale of commercial efficiency.[116] (Emphasis Supplied)

Schultz explains that horizontal fragmentation is driven by rationale of commercial efficiency. This is achieved by constitution of legal systems which are transnational and largely autonomous of State control. He cites the example of eBay's dispute resolution mechanism.[117] The objective of eBay's dispute resolution mechanism is to avoid the jurisdictional questions posed by the application of state law. On the other hand vertical fragmentation is a result of the forces of territorialism. It reflects concerns of public policy and the protection of local values, e.g., the *Yahoo!* case. There is vertical fragmentation of the internet by states exercising greater control over web based information flows within (and into) their territory based on local values and preferences. The latter has been triggered by a variety of factors including libel originating in distant countries, online casinos, domain name cyber squatting, hate speech websites and so on. What Schultz also effectively demolishes is the myth that the internet cannot be regulated.

The jurisdiction sought to be exercised by domestic courts over foreign defendants depends to a large extent in precisely 'locating' their presence in the physical terrain, if that is at all possible. It appears that the French Court hearing the *Yahoo!* case did advert to the possibility of using 'geolocation' technology to block viewership of the website to specified group of people based on their geographical location. The idea was that no French national in France should be able to view the Nazi memorabilia on display on the Yahoo! website. The French court was informed that this was technically feasible. However it is pointed out that this is not useful in localizing the activity since the puzzle remains whether the customers initiated the on-line activity by reaching out to access the commercial website or vice versa.[118]

The anxiety of countries and their courts to protect local citizenry from commercial or content-based harm while at the same time not wanting other countries to exert the same authority over its citizens is not unique. The differing policy priorities of countries defy the formulation of a uniform set of laws or codes to regulate activity on the internet. In purporting to answer Lawrence Lessig's question as to why some other court would want to enforce Minnesota's anti-gambling laws, Michael Geist answers:

---

[116] *Supra* note 70.
[117] *Supra* note 70.
[118] *Supra* note 3.

> The answer is that they would not if this were the only regulation at stake. Minnesota wants to protect its citizens from gambling, but New York may want to protect its citizens against the misuse of private data. The European Union may share New York's objective; Utah may share Minnesota's. Each state has its own stake in controlling certain behaviors, and these behaviors are different. But the key is this: the same architecture that enables Minnesota to achieve its regulatory end can also help other states achieve their regulatory ends. And this can initiate a kind of quid pro quo between jurisdictions.[119]

Any attempt at codifying 'uniform' norms to govern internet transactions will have to account for the inevitable attempts by states to assert territorialism on the basis of the need to protect local values and local commerce.

VI

CONCLUSION

An oft repeated quote in the context of the internet is that of Judge Nancy Gertner in *Digital Equipment Corp. v. Altavista Technology*:[120] "The internet has no territorial boundaries. To paraphrase Gertrude Stein, as far as the internet is concerned, not only is there perhaps 'no there, there', the 'there' is everywhere where there is internet access."[121]

This article traced the difficult and different paths that common law courts traversed in trying to formulate a definitive test which would lend legal certainty in tackling the complex problem of courts exercising jurisdiction in disputes arising out of activities on the internet. The problem is perhaps compounded by the fact that the technology which is rapidly changing is at least two steps, if not more, ahead of the law. The 'catch up' by the law appears as of now a mirage.

There can be no doubt that Indian courts will increasingly be called upon to exercise jurisdiction over foreign or extra territorial defendants engaged in internet transactions. And it is predictable that the Indian courts, even while they familiarize themselves with the complex nature of the problem, will continue to rely upon the law developed by the common law courts elsewhere.[122] It

---

[119] *Supra* note 9.
[120] 960 F. Supp. 456 (D. Mass. 1997).
[121] *Id.* at 462.
[122] The applicability of the *Banyan Tree* tests to non-IPR contexts, like torts and crimes is yet to be tested. In any event, it will not be surprising if the tests evolved in the context of enforcement and protection of IP rights are found inappropriate in other contexts.

appears that just as the technology is by and large a borrowed one, the law in relation to it will also inevitably be that.[123] There is scope and need for developing indigenous law. If in the area of IPR, Indian statutory law has been made to conform to the requirements of international law, it is hard to imagine that the position will be any different when it comes to the law governing e-commerce. While getting the law to cope with the technological changes in the use of the internet will be a formidable challenge, what can happen is that we may be irreversibly heading towards erecting more cyber borders, which can in turn generate a whole slew of law avoidance technologies. These concerns are the beginning in what predictably will be a long term engagement for law makers and those associated with the enforcement of law.

[123] The IT Act talks of electronic evidence, the certifying process and the authorities involved in that process and lists out the various offences constituting cyber crime including cyber pornography, cyber terrorism and violation of privacy and prescribes punishments for those offences. Interestingly, section 1(1) states that it extends to the whole of India and "applies also to any offence or contravention thereunder committed outside India by any person." While this provision may arguably be interpreted as an assertion of 'universal jurisdiction' over cyber crimes committed anywhere in the world by any person, the IT Act offers little guidance on e-commerce transactions.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 6, 2010

BALANCING ONLINE PRIVACY IN INDIA

Apar Gupta[*]

ABSTRACT

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

TABLE OF CONTENTS

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

I

INTRODUCTION

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

---

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

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

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

[4] *Supra* note 1, at ¶ 132.

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

II

THE RIGHT TO PRIVACY RECENTLY

A. THE TAXONOMY OF PRIVACY

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

B. LIMITED RECOGNITION OF HARMS

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

III

ONLINE PRIVACY: PAST, PRESENT AND ABSENT

A. INFORMATION GATHERING

1. General rules for information gathering

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

---

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

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

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

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

[61] *Supra* note 48.

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

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

2. Section 69 of the Information Technology Act, 2000

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

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

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

---

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

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

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

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

[68] *Id.*

[69] *Supra* note 48.

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

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

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

B. INFORMATION PROCESSING

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

C. INFORMATION DISCLOSURE/DISSEMINATION

1. Conventional treatment of information disclosure/dissemination

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

---

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

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

---

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

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

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

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

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

[83] *Supra* note 80.

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

[85] *Supra* note 81.

[86] *Supra* note 82.

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

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

2. Protection against online dissemination

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

---

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

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

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

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

IV

THE LIMITATIONS OF THE PRESENT PRIVACY REGIME

A. DESIGN DEFECTS IN THE PRESENT SURVEILLANCE REGIME

1. Lack of incentive, a lack of procedure

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

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

---

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

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

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

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

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

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

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

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

2. Absence of an effective injury discovery and redressal system

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

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

---

[97] *Supra* note 48.

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

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

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

B. A DEEPER CUT AT PRIVACY

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

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

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

---

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

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

C. ABSENCE OF WIDE DATA PROTECTION STANDARDS

1. Limited protection against private privacy risks

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

2. Non-recognition of the harm of information processing

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

---

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

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

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

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

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

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

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

V

CONCLUSION

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

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

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

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

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

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 6, 2010

POLICY-MAKING, TECHNOLOGY AND PRIVACY IN INDIA

Subhajit Basu[*]

ABSTRACT

There is a preconceived assumption that privacy laws in India are notoriously weak. This unquestioned assumption is based on a paradigm that does not take into consideration that the conception of privacy in India is influenced by its 'culture of trust.' Unfortunately, rather than looking into the specific societal, political and economic factors triggering the controversy, privacy researchers in the West have constantly varied the meaning and extent of the 'right to privacy' to bolster their argument. This article offers an explanation for why 'umbrella' data privacy legislation similar to the E.U. Data Protection Directive should not be enacted by India. This article further evaluates the argument that one's private sphere is subjective and depends on one's culture, environment and economic condition.

I

INTRODUCTION

This paper critically analyses India's statutory requirements regarding privacy and compares those requirements with the privacy culture established in the West in terms of the texture of the concept of privacy in these distinctly different social and cultural settings. Unfortunately, rather than looking into the specific societal, political, and economic factors triggering the controversy, privacy researchers have constantly varied the meaning and extent of the 'right to privacy.' Most of the definitions of privacy employed are culturally and historically biased in favour of the West and do not take into consideration other socio-historical contexts. What interests me more than the reasoning and the theoretical evidence behind the controversy is the value of looking at how those issues that vex people in the West arise in a different cultural context. Such examinations generate respect and a healthy curiosity.

In addressing privacy as an instrumental notion within social and cultural contexts, we must recognise that people perceive privacy and their 'reasonable expectations' of privacy in a way that has allowed those expectations to change in tandem with ongoing cultural, social and

[*] Senior Lecturer in Cyber Law, School of Law, University of Leeds.

technological changes. While not denying the importance of protecting privacy, this paper presents two plausible explanations for the difference in privacy concerns between India and the Western countries. First, the differences reflect and relate to differences in cultural values (for example the Indian culture of trust) and secondly, the role of privacy rights as embedded in the Indian constitutional tradition.

While critics have argued that privacy laws in India are notoriously weak because of the absence of a comprehensive legislation, the reality is somewhat different. I would argue that this unquestioned assumption is based on a paradigm that does not take into consideration that the conception of privacy in India is quite different from the Western conception of the same right. Firstly, the Indian perception of the word 'privacy' refers to privacy in terms of personal space and subjects.[1] Secondly, even in the West it is not clear what is protected, what is believed to be protected, what is actually protected and what is not protected in terms of privacy. In the course of this paper, I will further argue that one's private sphere is subjective and depends on one's culture, environment and economic condition. The reality of living in a welfare society is that we are living in the era of social reconstruction. It is common for theorists and advocates of privacy to agree that while privacy is an important interest, it must also be balanced against other competing interests. Hence, instead of looking at privacy as a right, I shall refer to privacy as an interest which can be invaded for 'social good.'[2]

My interest in the problem of privacy in the Indian context is motivated by the hysterical reporting of popular mass media in the West on the risk to privacy and data security posed by 'offshore outsourcing' to India. It is undeniable that identity theft and credit card fraud are huge problems

[1] 48% of the subjects in India related privacy to physical, home and living spaces, but only 18% of the subjects in the United States related privacy to these concepts. 89% of the subjects in the United States disagreed with the statement that 'Data security and privacy is not really a problem because I have nothing to hide', but only 21% of the subjects in India disagreed with the above statement. Regarding privacy issues in relation to technology, a minority (21%) of the subjects in India expressed concern about keeping computerised information secure, but 79% of the subjects in the United States expressed such a concern. While responding to the above question, 25% of the subjects in the United States expressed concern about identity theft, but the topic remained unaddressed by the subjects in India. *See* PONNURANGAM KUMARAGURU ET AL., PRIVACY PERCEPTIONS IN INDIA AND THE UNITED STATES: AN INTERVIEW STUDY (2005), *available at* http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf.

[2] The Government of Australia has recently relaxed privacy laws to pass on personal information about half a million foreign students across the country to the police in order to help them investigate whether the recent attacks on foreign students, including Indian students, were racially motivated. According to Australian Privacy Commissioner Karen Curtis, the release of students' names and ages, held by the Department of Immigration, was a one-off decision in the national interest. *Oz relaxes laws to pass details of foreign students to police*, ECON. TIMES, May 20, 2010, *available at* http://economictimes.indiatimes.com/news/politics/nation/Oz-relaxes-laws-to-pass-details-of-foreign-students-to-police/articleshow/5953900.cms.

globally; however, there is no evidence, to suggest that consumer data is at any greater risk in India than in the UK[3] or the US,[4] nor is there any evidence to prove that consumers in highly regulated countries trust the companies collecting their personal data,[5] hence it is unjustified to stigmatize one particular country or group of countries unnecessarily. The intention of this article then is to offer an explanation for why India's conception of privacy is dominated by the public-private dichotomy and has implicitly or explicitly affected the agenda for privacy theory by placing some issues in the limelight and others backstage.

II

PRIVACY EFFICACY

Social patterns and values today are too diverse, decentralised, and purposefully different to provide a foundation for general rules of discourse at the level of specificity required for the protection of privacy. This does not imply that a legal concept of privacy should be disregarded; instead, protection can be defined as specifically or as generally as the legislature chooses by taking into consideration the cultural context and allow its contours to fit within the social and economic conditions. It is important that we explore these foundations for the purposes of identifying the assumptions, assessing its justifications, and analysing the paradoxical effects of India's privacy policies.

The idea of privacy is intimately connected with the conception of liberty, justice, human dignity, individuality and family life. Although the concept of privacy is a longstanding phenomenon, codification of privacy as a right is rather new. Further, as societies go through a fundamental transformation, it also creates the need for re-conceptualising the right to privacy. The question arises in terms of how far it should be protected and against what? Most scholars tend to define privacy within the confines of their specific research. For example, privacy as the 'right to be let

---

[3] The UK's Information Commissioner's Office reports that nearly 100 data breaches were reported in the three months since October 2008. The number of data breaches has increased by almost 36% as compared to the previous year – 376 data breaches at the end of January 2009 as compared to 277 data breaches at the end of October 2008. It thus appears that personal information is now lost more than once a day on average. *See* Press Release, Information Commissioner's Office, Data breaches reported to ICO (Feb. 9, 2009), *available at* http://www.ico.gov.uk/upload/documents/pressreleases/2009/data_breaches_ico_statement20090209.pdf; *see also* Richard Thomas, UK Information Commissioner, Speech to the RSA Conference Europe (Oct. 29, 2008), *available at* http://www.ico.gov.uk/upload/documents/pressreleases/2008/rsa_speech_oct08_final.pdf.

[4] *See* Joseph Cannataci & Jeanne Bonnici, *The UK 2007-2008 Data Protection Fiasco: Moving on from bad policy and bad law?*, 23 INT'L REV. L. COMPUTERS AND TECHNOLOGY 47 (2009).

[5] *See* Press Release, IBM, E-businesses exhibiting privacy leadership get the sale, according to new IBM consumer study on privacy (Nov. 8, 1999), *available at* http://www-03.ibm.com/press/us/en/pressrelease/1979.wss.

alone' is a rather simple concept and cannot be used in a meaningful way. Such a narrowly constructed conception of privacy in obvious ways is restricted in its utility. Gavison argues that, 'not letting people alone' cannot readily be described as an invasion of privacy.[6] I argue that what counts as a right to privacy, then, has the potential of having important consequences on a variety of scales. Hence, inevitably, the demands of the modern society and technological changes require a redefinition of the right to privacy.

Does everybody in society get equal protection in terms of privacy and how much privacy is desirable? Every individual should have the same claim to privacy. Thus, one individual's exercise of privacy must submit to the equal claim of every other individual to the same exercise. However, in reality, this does entail some loss of privacy for everybody. Gavison argues that there is a loss of privacy when others obtain information about an individual, pay attention to him or her, or gain access to him or her. She suggests that the concept of privacy consists of a complex combination of three elements – secrecy, anonymity and solitude.[7] While these elements are independent of each other, they are also related. Privacy therefore consists of the individual's control over access to, and information about, himself or herself.[8] An individual who chooses to disclose certain aspects of his or her private life cannot experience a loss of privacy on the ground that others gain access to him or her. On the contrary, if the individual chooses not to allow others to gain access to himself or herself, or his or her personal information, then any intrusion into his or her private affairs or a disclosure of his or her personal information would violate his or her right of privacy. Therefore, the variation in the quality of privacy is dependent on the extent and frequency with which an individual is 'exposed' to the public. It seems reasonable to suppose that, as with other social values, some inequality in the distribution of privacy does exist.[9]

It is with this purpose that I distinguish 'informational privacy' from 'decisional privacy.' The focus of decisional privacy is on freedom from interference when making certain fundamental decisions. In contrast, informational privacy is concerned with the use, transfer, and processing of personal data generated in daily life. "The extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others'

---

[6] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 437 (1980).
[7] *Id.* at 428.
[8] James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFF. 323, 326 (1975).
[9] COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 35 (2003).

attention."[10] This approach has been criticised on the ground that if a loss of privacy occurs whenever any information about an individual becomes known, then the concept of privacy loses its intuitive meaning. Such a proposition leads to the awkward result that any loss of the solitude of, or information about, an individual becomes a loss of privacy.[11]

Contrary to approaches like Gavison's, Wacks[12] argues that a limiting or controlling factor is required. He points out that although focusing attention upon an individual or intruding upon his solitude is inherently objectionable in its own right, our concern for the individual's privacy in these circumstances is strongest when the person is engaging in activities that we would normally consider private. He suggests that the protection afforded by the law of privacy should be limited to information "which relates to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict its collection, use, or circulation."[13] If the right to privacy would be recognised by law, it would extend only over a limited, conventionally designated, area of information,[14] "symbolic of the whole institution of privacy."[15] Hence, it can be argued that access to personal information is a necessary but not sufficient condition for it to be defined as falling within the scope of privacy. What is further required is that the information must be of an intimate and sensitive nature, such as information about a person's sexual proclivities, but the content may also differ considerably from society to society.

III

PRIVACY IN INDIA'S CULTURAL PERSPECTIVE

The existence of multiple cultures and philosophies prompts questions regarding appropriateness, hegemonic relations, and privileging one culture over another. Before the debate can begin, we need to understand that each nation has a distinctive, influential, and describable culture;[16] hence, each country, from its own unique background, determines the ways in which its citizens express

---

[10] *Supra* note 6.

[11] RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 15-18 (Clarendon Press 2003) (1993).

[12] *Id.* at 26.

[13] *Id.* at 26.

[14] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998).

[15] Charles Fried, *Privacy,* 77 YALE L.J. 493 (1968).

[16] Culture is "the interactive aggregate of common characteristics that influences a human group's response to its environment. Culture determines the identity of a human group in the same way as personality determines the identity of an individual." *See* GEERT HOFSTEDE, CULTURE'S CONSEQUENCES: INTERNATIONAL DIFFERENCES IN WORK-RELATED VALUES 25-26 (1980).

and understand the same concept.[17] What makes Indian culture special is the concept of the autonomous non-distinctive individual not living within society. When it comes to the 'man-in-society,' the Indian view is not unique. Indeed, the view is a prototypical and lucid expression of a widespread mode of social thought,[18] but it does diverge quite considerably from the 'natural man' tradition of Western social thought.[19] The Western "autonomous individual imagines the incredible, that he lives within an inviolate protected region (the extended boundaries of the self) where he is 'free to choose'."[20] I will contrast this with the alternate conception, the holistic culture of India, which seems to embrace a socio-centric conception of the relationship of the individual with society. According to Hofstede,[21] India is a collectivist society with a lower Individualism Index (IDV)[22] and a higher Power Distance Index (PDI)[23] as compared to the UK or the US, which are individualist societies with higher[24] IDV where an individual's importance is at least equal to, if not greater than, the importance of the collectivity. Hofstede has shown that individuals in collectivist societies have more faith in other people than those in individualist societies.[25]

A country's cultural values are known to affect a population's attitudes toward privacy and are associated marginally with its regulatory approach.[26] What then are the influences of cultural specificity on privacy? Western societies came to view privacy as an important value that gave rise to a privacy interest or right recognised by law or social convention.[27] Unsurprisingly, Indian cultural values also play a significant role in shaping attitudes about privacy. It is in the interest of the Indian society that both the individual rights aspect of privacy as well as the social value of

---

[17] *Id.* at 25-27.

[18] *See* D. W. Murray, *What is the Western Concept of the Self? On Forgetting David Hume*, 21 ETHOS 3 (1993).

[19] Richard A. Shweder & Edmund J. Bourne, *Does the Concept of the Person Vary Cross-Culturally?*, *in* CULTURE THEORY: ESSAYS ON MIND, SELF, AND EMOTION 158-199 (Richard A. Shweder & Robert A. LeVine eds., 1984).

[20] *Id.* at 182.

[21] Hofstede developed a number of cultural values indices to measure cultural differences between societies. He identified five distinct dimensions of human behavior that characterize a culture: (1) power distance, (2) uncertainty avoidance, (3) individualism/collectivism, (4) masculinity/femininity, and (5) long-term or short-term orientation. GEERT HOFSTEDE, CULTURE'S CONSEQUENCES: COMPARING VALUES, BEHAVIOURS, INSTITUTIONS, AND ORGANIZATIONS ACROSS NATIONS 79 (2001).

[22] The Individualism Index (IDV) measures the extent to which a society tends to emphasize individual rights as compared to collective goals. *Id.* at 79.

[23] 'Power distance' is defined as the way in which a culture approaches and accepts inequality in status, prestige, wealth and power. *Supra* note 21.

[24] *Supra* note 21.

[25] *Supra* note 21.

[26] *See* Sandra J. Milberg et al., *Information Privacy: Corporate Management and National Regulation*, 11 ORG. SCI. 35, 39 (2000).

[27] Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES 431 (2003).

privacy is preserved. However, the degree of need for such preservation would vary from individual to individual and would make it highly subjective. While it is a common practice in the UK for general practitioners (GPs) to not discuss patient information relating to the wife with her husband, such discussion is quite common in India, where GPs regularly discuss such issues with the husband or other members of the family. Interestingly, I sometimes find myself contradicting my own thoughts because I am torn between the dichotomy of the Western conception of total control over information and the Indian culture of trust. The result is two worlds with clear rules. However, problems arise because these diverse cultures are interacting with each other, yet each culture is retaining its own set of values and beliefs.

Are any aspects of life inherently private and not just conventionally so? As discussed in the previous section, one of the interests most commonly associated with privacy is the interest in controlling access to, and dissemination of, information about oneself. Hence, not surprisingly, in India and probably in every other place in the world, people recognise that certain types of information about oneself are privileged. However, in India, the people's perception about 'privacy' is predominantly associated with 'secrecy' and 'personal space' and how people relate to, communicate and share each other's professional, familial and personal information but it is not about the economic value of that information. Indeed, the concern for 'bodily privacy' is amongst the most ancient and deeply traditional concerns of both Hindu and Muslim cultures. In *Ganeshi Lal v. Rasool Fatima*,[28] the court found that Indian women have always been protective of their privacy in their homes. It is the archetypal private space. Privacy inside the house is a right of every woman and much more so for a woman who has inhibitions by custom or religious notions against appearing in public and keeps herself in seclusion by observing 'purdah.'[29] In *Basai v. Hasan Raza Khan*,[30] the court recognised 'purdah' as the basis of this right and held that it entitled the owner of one property to compel the owner of another to modify the design or architecture of his property so that the woman residing in the dominant tenements could be kept in 'purdah.' According to the court, the right is based on 'natural modesty or human morality.' The court, however, held that the customary right to privacy can be claimed only in respect of apartments which are generally occupied and used by females and does not extend to apartments ordinarily used by males, the basis of the customary right of privacy being the 'purdah' system which was

[28] A.I.R. 1977 All. 118 (India).
[29] 'Purdah' literally means curtain. It is the practice of preventing women from being seen by men. This takes two forms: physical segregation of the sexes, and the requirement for women to cover their bodies and conceal their form. Purdah exists in various forms in the Islamic world and amongst Hindu women in some parts of India.
[30] A.I.R. 1963 All. 340 (India).

confined to the protection of 'purdanashin' women and those parts of a house which were ordinarily occupied by females.

It can be further argued that custom once established does not extend only to women who are in the habit of observing 'purdah,' but all women are entitled to this specific degree of privacy. Although it is equally true that the right of privacy cannot be extended to an oppressive length, a variety of social, economic and technological changes in India, have, over the years, seemed to widen the arena within which the presumption of a right to privacy ought to operate. Over this period, the area within which private activities can take place has also been extended beyond the home. In the recent *Naz Foundation* case, the Delhi High Court held that the right to privacy protects a "private space in which man may become and remain himself."[31] The judges predicated their application of the right to privacy in this case with a discussion of the concept of 'dignity' and its presence in the Indian Constitution. The court observed that "at its least, it is clear that the constitutional protection of dignity requires us to acknowledge the value and worth of all individuals as members of our society. It recognizes a person as a free being who develops his or her body and mind as he or she sees fit. At the root of dignity are the autonomy of the private will and a person's freedom of choice and action."[32] The decision articulates a unique, non-spatial and portable understanding of privacy that extends beyond 'place' into 'person.' It is potently clear that the Indian conception of privacy is dominated by factors such as the rights of the family, the 'purdah' observed by women and the belief that such intrusion affects the modesty, dignity or decency of a person. However, it is not sufficient in conceptual terms to treat an invasion of privacy as an affront to human dignity alone, as it is possible that an individual's dignity could be offended without his privacy being invaded.

Interestingly, similar findings regarding public perception of privacy were reported in the two surveys published by the School of Computer Science at Carnegie Mellon University.[33] Both surveys are quite revealing in the sense that they vividly underline the great gap that separates the Western perception of privacy and the predominant perception in India. The two surveys found

---

[31] Naz Foundation v. Government of N.C.T. of Delhi & Ors., 160 (2009) D.L.T. 277 (India) (*Per* A. P. Shah, C.J. & S. Muralidhar, J.). The Delhi High Court decided to strike down provisions that criminalised consensual homosexual sexual conduct on the grounds of invasion of privacy.

[32] *Id.* at ¶ 26.

[33] *See* Ponnurangam Kumaraguru & Lorrie F. Cranor, *Privacy in India: Attitudes and Awareness*, *in* PROCEEDINGS OF THE 2005 WORKSHOP ON PRIVACY ENHANCING TECHNOLOGIES (PET 2005: 30 MAY - 1 JUNE 2005, DUBROVNIK, CROATIA), *available at* http://lorrie.cranor.org/pubs/PET_2005.html; *see also supra* note 1.

that typical responses by Indians when asked about privacy were 'privacy for me is my personal territory' and 'personal privacy.'[34] However, the surveys also do not show that privacy is 'less valued' in Indian culture. These surveys completely undermine a familiar canard about non-Western societies;[35] that they do not ascribe the same value that Western societies do to privacy.[36] It confirms that Indians are more concerned with a different dimension of privacy and so ascribe a greater value to protecting the concerns that fall under the same.[37] It further re-emphasises that privacy is a highly subjective value. Public policy and law can only establish rules, principles and procedures if and when the same are required or demanded (e.g. if there are concerns about information privacy then governments can become more involved because individuals are more likely to call for stronger privacy laws) but it is also up to individuals to assert their own privacy interests and claims. Hence, there is a positive statistical relationship between nationality, privacy concerns and privacy regulations.[38]

Ethical relativism postulates that "morality is relative to the norms of one's culture"[39] and that "whether an action is right or wrong depends on the moral norms of the society in which it is practiced."[40] We cannot apply a universal code of ethics and laws across the world given our different cultures and beliefs. The overriding question is which set of ethics and beliefs should be

---

[34] With regard to cultural prescriptions and privacy, Kumaraguru & Cranor refer to the lack of an explicit privacy concern be it amongst family members running a family business or in the work place. There exists a certain amount of naiveté about databases of personal information traded and sold between trading companies. *Id.*

[35] For example, the concept of privacy in Thailand is 'collective' and different from the more 'individual' Western conception. Buddhism, which is practiced by most people in Thailand, does not recognize human beings as possessing inherent rights endowed at birth in the sense of human rights such as the right to privacy. So, the word 'privacy' has different cultural understandings. *See* Krisana Kitiyadisai, *Privacy Rights and Protection: Foreign Values in Modern Thai Context*, 7 ETHICS & INFO. TECH. 17 (2005). From a Chinese perspective, privacy is also not seen as an 'intrinsic good' but as an 'instrumental good', meaning that the Chinese do not view privacy as essential, although they consider the concept to be important. *See* Lü Yao-Huai, *Privacy and Data Privacy Issues in Contemporary China*, 7 ETHICS & INFO. TECH. 7 (2005).

[36] *See* Martha C. Nussbaum, *Is Privacy Bad for Women? What the Indian Constitutional Tradition can teach about sex equality*, 25 BOSTON REV. 42 (2000).

[37] Debate about policies, community expectations, industry codes and legislation has primarily addressed data collection/handling by government agencies rather than the private sector. In particular, it has centred on political surveillance and censorship, reflecting the public outlook about civil society and individual rights.

[38] Milberg and Westin found that countries with either 'no privacy regulations,' or the strictest model of privacy regulations were associated with significantly lower information privacy concerns, and countries with moderate regulatory structures were associated with higher aggregate levels of concern. *See* ALAN WESTIN, PRIVACY AND FREEDOM (1967); *see also* Sandra J. Milberg et al., *Values, Personal Information Privacy, and Regulatory Approaches*, 38 COMM. OF THE ACM 67 (1995).

[39] Claire Andre & Manuel Velasquez, *Ethical Relativism*, 5 ISSUES IN ETHICS (MARKKULA CENTRE FOR APPLIED ETHICS) (1992), *available at* http://www.scu.edu/ethics/publications/iie/v5n2/relativism.html.

[40] *Id.*

used to set rules and laws? History itself is littered with examples of 'uninvited cultural invasion and overthrow,'[41] where values and assumptions were adopted with little questioning.

What results from this discussion, I contend, is not a choice of one over the other but rather a dualism. To me, a more effective argument for the cultural relativity of privacy conceptions would be structured differently. Any reasonably developed culture has a basic understanding of privacy based around a 'minimal conception.'[42] It is important to note here that this 'minimal conception' is shared by all cultures. What is then required is multiple matching between these variations in cultures and their respective privacy conceptions.[43] Hence, the policy need not be common, but neither should it be singular, it should rather be a conjunction of contexts that requires the norms of each context to be respected and protected from homogenisation.

What has been the influence of the 'technological culture' of information technology? Information technology has managed to streamline and amplify the collection and analysis of data as well as its use in decision-making. It is true that because of this we are now producing, processing, storing, automatically sorting, extracting and comparing vast amount of data like never before.[44] It appears to provide a panacea of observation, analysis, prediction, and control for those who wish to reduce uncertainty and unpredictability. As I have mentioned before, in an information society, those who send information and those who filter information have economic power and also have the power to influence and shape privacy and probably will ultimately control the privacy of individuals. But it has also created vulnerability. In the case of India, at the present moment, it seems that this vulnerability is the lack of clarity regarding the classification of information, which is making the management of information much more complicated. In the next section, I will discuss if it is in the economic interest of India to adopt a definitive privacy policy, specifically in the context where privacy is perceived to be threatened by new technologies.[45] The focus of the section is on the intersection of privacy and economics.

---

[41] TREVOR HAYWOOD, INFO-RICH INFO-POOR: ACCESS AND EXCHANGE IN THE GLOBAL INFORMATION SOCIETY 131 (1995).

[42] Masahiko Mizutani et al., *The Internet and Japanese Conception of Privacy*, 6 ETHICS & INFO. TECH. 121, 121-128 (2004).

[43] Different cultures will receive and interpret information differently regardless of the universal concepts which all people share. The same information will not produce the same understanding.

[44] A basic list of technologies that have the potential to impact privacy are: radio frequency identification, smart cards, location detection technologies including G.P.S., data mining technologies, surveillance technologies and biometrics.

[45] India's outsourcing industry is expected to earn revenues amounting to $50 billion by 2012. It is also expected to provide direct employment to 2 million workers by 2012. The outsourcing industry in India has grown at more than

IV

PRIVACY IN INFORMATION SOCIETY: ECONOMIC CULTURE

Cultures are not independent of economic and technological forces. The interplay between technological development and cultural curiosity is helping to define the information society. The information economy continues to drive Indian commerce.[46] Indian outsourcing and information technology companies have created hundreds of thousands of jobs in India,[47] the industry has completely revolutionised how consumers and businesses interact, transact and use information. Hence, the dilemma for India, which has a substantial interest in the development of information industries, is whether the country can completely ignore the Western, particularly the European, demand for specific data privacy legislation. Usually this dilemma is never stated so obviously but its existence is accepted nonetheless.

The internet is transforming critical sectors of the global economy and society, such as health care, energy, education, the arts and political life. In all these sectors, proper use of personal information can play a critical, value-adding role, so establishing trust and assuring flexibility is vital. The economic significance of privacy in an information society is dependent on how much people value their privacy. The earliest economic analyses of privacy focused on the efficiency of markets for personal information. Almost all developed countries have grappled with the trade-off between open access to information which enables economic efficiency and an individual's right to privacy. My objective here is to briefly evaluate the utility of allocating the value of personal information. Laudon argues that market-oriented mechanisms based on individual ownership of personal data could enhance personal data protection.[48] If 'personal data markets' were allowed to function more effectively, there would be less privacy invasion.

Under the traditional economic model, competitive market forces will generally deliver an economically efficient outcome. Hence, an efficient amount of information sharing will occur up to the point where the economic benefits of information sharing are balanced against the associated costs. Specifically, if the economic value created by information sharing exceeds the value derived from privacy, theory maintains that the economically efficient outcome would be to share information. In contrast, if the economic value generated by private parties from access to

---

30% a year for five years since 2003. *India's outsourcing revenue to hit $50 bn*, FIN. EXPRESS, Jan. 29, 2008, *available at* http://www.financialexpress.com/news/indias-outsourcing-revenue-to-hit-50-bn/266661.

[46] *Id.*

[47] *Supra* note 45.

[48] Kenneth C. Laudon, *Markets and Privacy*, 39 COMM. OF THE ACM 103 (1996).

personal information does not exceed the individual benefit from privacy, then economic efficiency dictates that information is not be shared.[49] In other words, individuals will provide personal information as long as they perceive that adequate benefits shall be received in return – i.e. benefits which exceed the perceived risks of information disclosure.[50] So long as individuals undervalue their personal information relative to its market value, there will be a buyer for it in today's information hungry economy.[51] This perception is important from a developing country perspective because there is a direct relationship between micro-economics, the use of personal data and the increase in contribution to the Gross Domestic Product (GDP), national competitiveness and economic growth; this means that governments should evaluate the practical implications for businesses before introducing stringent privacy regulations protecting personal information.

Milberg found a significant and positive relationship between concerns about information privacy and the level of government involvement in the regulation of privacy.[52] There can be various situations involving both consequential and direct externalities where the commitment to protect privacy increases welfare. Specifically, certain analyses of behaviour-based price discrimination in competitive settings show that businesses may benefit from the privacy of personal information.[53] It is worth remembering in this respect that the economic analysis of consequential externalities suggests that whether and how privacy increases welfare depends on the particular circumstances.[54] The economic analysis of consequential externalities suggests that whether and how privacy increases welfare depends on the particular circumstances. Clearly, a free market for personal information will not provide an economically efficient outcome. Hence, from an economic point of view, the question is whether privacy regulation is more likely to increase welfare in the context of non-productive information as compared to productive information. Understanding how the private sector uses personal information can reveal how policies and regulations to protect privacy can be properly tailored; this means that the contentious debate about privacy regulation may have

---

[49] *See* Hal R. Varian, *Theory of Markets and Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997), *available at* http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm.

[50] *See* Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyberbolic Discounting*, *in* THE ECONOMICS OF INFORMATION SECURITY 5 (J. Camp & R. Lewis eds., 2004), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti_grossklags_eis_refs.pdf.

[51] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1465 (2000).

[52] *Supra* note 26, at 39-57.

[53] Drew Fudenberg & J. Miguel Villas-Boas, *Behaviour-Based Price Discrimination and Customer Recognition* (2005), *available at* http://www.haas.berkeley.edu/~market/PAPERS/VILLAS/surveypaper.pdf.

[54] K. L. Hui & I. P. L. Png, *The Economics of Privacy*, *in* HANDBOOKS IN INFORMATION SYSTEMS (Terrence Hendershott ed., 2006).

been misdirected. Finally, it is undeniable that economic diplomacy has now become pivotal part of Indian foreign policy, but economic policy cannot be detached from the socio-political and cultural reality of the country.

V

INDIAN JUDICIAL RECOGNITION OF RIGHT TO PRIVACY

Despite pressure from internal and external sources, India has traditionally shown a general unwillingness to adopt data privacy laws.[55] I have stated before that there is a significant and positive relationship between concerns about privacy and the level of government involvement in the regulation of privacy.[56] Thus, differences in political systems and legislation in various countries can be interpreted as consequences of societal value differences and the degree to which members of a society look to the government to remedy social issues.[57] In the United States[58] and, until recently, Canada and Australia, privacy regulation has tended to be targeted and sector specific, and to be aimed mainly at the public sector. This sectoral or voluntary approach contrasts with the omnibus approach, to both the public and private sectors, used by the European Union. The right to privacy in India is a peculiar blend of constitutional, customary and common law rights scattered across various legal fields. As a customary right, it is treated as an easement. As a part of the constitutional right to life and liberty, it is considered to be an illustration of the prerogative development of human rights and basic freedoms.

The analysis made earlier in the article emphasises that India's history has not been plagued by privacy abuses and identity theft. It is true that there is a positive association between the level of privacy concern and the level of governmental involvement in the management of privacy but I am inclined to argue here, however, that India's recent general reluctance to legislate for data privacy protection may be deeply rooted in its colonial past. A country's 'legal origin' significantly affects the subsequent evolution of its legal rules. Due to the greater constitutional independence of the judiciary in 'common law' legal systems, such legal systems are thought to exhibit both a greater

[55] At the time of writing this article, India still has not adopted a legislation which explicitly governs the protection of personal data. Data privacy protection was discussed in the late 1990s as part of the formal discussions regarding the provisions to be included in the proposed information technology legislation, but the Information Technology Act, 2000 did not include provisions in relation to data privacy.

[56] *Supra* note 26, at 35-57; Milberg et al., *supra* note 38, at 65-74.

[57] *Supra* note 26, at 35-57.

[58] The US privacy framework is composed of sectoral laws combined with constitutional, statutory, regulatory and common law protections, in addition to industry self-regulation. Sectoral laws govern the handling of personal data considered to be most sensitive in nature.

degree of adaptability than 'civil law' legal systems through their greater reliance on 'bottom up' rule-making by the judiciary as opposed to 'top-down' codifications, and a lesser degree of susceptibility to corrosion by rent-seeking politicians and bureaucrats.[59] Although India is described as a common law country having inherited a common law legal system from the UK, many of its laws were, in fact, codified during colonial rule, which was driven by an agenda of distrust that resulted in an array of rules and regulations that were almost impossible to uphold. In post-independence India, these were then overlaid with more legislation when the government implemented a socialist reform agenda encompassing all areas of commercial activity resulting in an obstructive bureaucracy[60] and relentless overregulation. The legal system that India inherited from the colonial era suffers from three defects – delay, cost and glorious uncertainty in the final outcome of any litigation. It is a maze of complex procedures together with a multiplicity of laws. In the wake of this pattern, businesses in the private sector had to wait months or even years for a response to their requests for government approval of entrepreneurial projects at many times waiting in vain.[61] It was not until the 1990s that this overly-stifling quagmire of excessive government control started to get dismantled, and since then, there have been rapid and far-reaching law reforms.[62]

The repressive environment which dates from the colonisation of India and has lasted through independence has caused an understandable fear of government regulation.[63] Furthermore, the nature of coalition politics in India, coupled with a very active judicial review process, means that enacting legislation is a slow and erratic process. Hence, the scepticism about legislation protecting data privacy is understandable. It has also provoked the questions of whether and to what extent, if at all, the current constitutional tradition provides privacy in India. Should it be supplemented to

---

[59] John Armour & Priya Lele, *Law, Finance, and Politics: The Case of India* (Eur. Corp. Governance Inst. (ECGI), Law Working Paper No. 107, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116608.

[60] Indrajit Basu, *India tries to root out bureaucratic corruption*, ASIA TIMES, Oct. 9, 2003, *available at* http://www.atimes.com/atimes/South_Asia/EH07Df01.html.

[61] GURCHARAN DAS, INDIA UNBOUND 216-218 (2002).

[62] The liberalising New Economic Policy of 1991 lead to a dramatic reconfiguration of the Indian economy. The motivating idea was to move from an economy controlled and planned by the state to one in which the private sector was to have a significant role, competition was to be encouraged, market-oriented mechanisms were to be developed, and government intervention was to be limited to the extent justifiably required. *See* JAGDISH N. BHAGWATI, INDIA IN TRANSITION: FREEING THE ECONOMY (1993); *see also* A. Panagariya, *India in the 1980s and 1990s: A Triumph of Reforms* (International Monetary Fund (IMF), Working Paper No. 3, 2004).

[63] In India, there is no sunset provision for statutes, and so, unnecessary statutes remain on the statute books till they are repealed. Some of these dysfunctional legislations have been repealed on the basis of the reports of the Law Commission of India which have been accepted by the Government of India. But several such statutes including some statutes from the British period are still cluttering the statute books.

manage privacy in the information society? Or is there a need for more radical changes in Indian law and policy to effectively address privacy concerns?

There is a substantial debate regarding whether a 'right to privacy' exists in India, how such a right is derived philosophically, and the extent to which such a right, if it does exist, is bounded. However, we should be asking an altogether different question: if we were to deny that people have a right to privacy, what would be the impact of this denial on the values that the Indian Constitution was designed to protect? Certainly, the Indian courts did not recognise any natural right to privacy and believed that such a right can be acquired only as a customary easement.[64] Indian courts have long acknowledged the relationship between privacy and information about persons, and have argued for limits on allowable practices of information gathering, analysing, and sharing as a means of protecting privacy, but all their efforts have primarily applied to intimate and sensitive information. How far have the Indian courts taken the fledgling right to privacy? Indian judges like the English judges have explicitly invoked such a right, though without taking the final step of creating a new legal right. The Allahabad High Court in *Nihal Chand v. Bhawan Dei*[65] had first recognised the independent existence of the right to privacy:

> the right to privacy based on social custom is different from a right to privacy based on natural modesty and human morality, the later is not confined to any class, creed, colour or race and it is a birth right of any human being and is sacred and should be observed.

The Indian Constitution does not expressly recognise the right to privacy but there is a strong belief that the Indian Constitution contains certain rights other than those that are expressly mentioned in its text. To establish the presence of such a right, it must be shown that the right in question is an integral part of an enumerated right upon which its existence depends. The rationale behind this formulation is simply that the enumerated right would be meaningless without providing for certain other rights by implication. Hence, the Supreme Court of India[66] accepted in 1964 that a right of privacy[67] is implicit in the Constitution under Article 21, which states, "no person shall be deprived of his life or personal liberty except according to procedure

---

[64] C. Krishna Murthy v. U. Rajlingam, A.I.R. 1980 A.P. 69 (India), ¶ 8.
[65] A.I.R. 1935 All. 1002 (India).
[66] India's independent judiciary, with the Supreme Court at the apex, has been a key feature of India's democracy throughout its existence. The role of the Supreme Court as the protector of individual rights is guaranteed under the Constitution of India. Basic individual rights are given constitutional protection as 'fundamental rights'. *See* INDIA CONST. arts. 12-35.
[67] Kharak Singh v. State of U.P., (1964) 1 S.C.R. 332 (India).

established by law."[68] The Supreme Court equated 'personal liberty' with 'privacy,' and observed that the concept of liberty in Article 21 was comprehensive enough to include privacy and that "nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy."[69] On the basis of this provision, the Supreme Court held that "those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law."[70] In the case of *People's Union for Civil Liberties v. Union of India*,[71] the Supreme Court held that the right to life and personal liberty under Article 21 includes the right to privacy and so improper telephone tapping violates Article 21.

At the time of the drafting of the Indian Constitution, the home was seen as the central locus of intimate activities, and hence as the place where the intervention of the government needed the strongest justification. Indian courts have thus interpreted the right to privacy as an implied fundamental right against state action. The perception of privacy as a fundamental right also changes depending on the person concerned and the context in which this right is being exercised. It is not viewed as an 'absolute' right, nor does it address 'information privacy.'[72] Indian case studies[73] also illustrate a significant tension between the contours of the right to privacy as against other rights and interests.[74] Even in its constitutional context, the meaning of privacy and how far the right to privacy extends remains unclear.[75] Somewhat unfortunately, the constitutional right to

---

[68] Madhavi Divan, *The Right to Privacy in the Age of Information and Communications*, 4 SCC (J.) 12 (2002).

[69] *Supra* note 67.

[70] *Supra* note 67; Gobind v. State of M.P., (1975) 2 S.C.C. 148 (India); State v. Charulata Joshi, (1999) 4 S.C.C. 65 (India).

[71] A.I.R. 1997 S.C. 568 (India).

[72] In the case of *State of Maharashtra v. Madhulkar Narain,* A.I.R. 1991 S.C. 207 (India), it was held that the 'right to privacy' is available even to a woman of easy virtue.

[73] This argument is supported by two widely debated cases of invasion of privacy in India. The first one is the DPS MMS scandal case in which Baazee.com CEO and Indian-born US citizen Avnish Bajaj was sent to jail for six days by a Delhi court. The focus of this case was not on the intrusion of privacy but the illegal distribution of the MMS clip on net. The police claimed that Baazee.com had listed the MMS clip on its website for sale and that the CEO did not make any efforts to remove it until prodded. The second case involved stealth video footage of an actor, captured by a media agency, invading privacy in the process and the actor found little recourse in law apart from being able to file a defamation suit.

[74] The Supreme Court has held that intrusions into privacy can be permitted and justified using legislative provisions, administrative/executive orders, and judicial orders. The court can compare the reasonableness and proportionality of the intrusion vis-à-vis the purpose of the intrusion. However, the Supreme Court did not take into account the possibility that the procedure established by law in India might be unjust or unreasonable. *See supra* note 67; *see also* Gobind v. State of M.P. (1975) 2 S.C.C. 148 (India); *see also* State v. Charulata Joshi, (1999) 4 S.C.C. 65 (India).

[75] In *M. P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300 (India), the Supreme Court held that the power of search and seizure does not violate the right to privacy because it is in the interest of the State. However, in *Menaka Gandhi v.*

privacy, although recognised in India and based on the comparative theoretical evaluation of Western and Indian legal systems for protecting privacy, is far more restrictive. It also cannot be denied that there is an uncertainty about the conceptual basis of privacy. However, I argue that although it is evident from the examination of the constitutional position and the history of the right to privacy in India that the right must be made subservient to national interest and national security at all times, recent Supreme Court decisions reflect conceptions of cultural and technological change and economic need.

Informational privacy, understood as data protection in the digital environment, is seen as an economic issue.[76] While the Supreme Court of India has recognised a general right to privacy, no general right relating to personal data protection has been developed to date. On evidence, the specific issue of enforcement, therefore, remains a problem. The absence of a general data protection legislation and the political philosophy of non-regulatory policies have translated into self-regulation and implementation of industry codes.[77] But surprisingly it has also forced India to deploy a more proactive approach that seeks to find legal solutions for data protection and data privacy in order to protect the economic interests of the country. This perspective acknowledges that in a globalised world, the preservation of the value of privacy is also closely linked with the economic development of the country.[78] From this perspective, informational privacy requires some degree of social and legal control.

The subject matter of data protection in India has been dealt with by the Information Technology Act, 2000, No. 21 of 2000, but not in an exclusive manner.[79] One can argue that the legislation

---

Union of India, A.I.R. 1978 S.C. 597 (India), it was held that it would not be enough to say that a violation of privacy would be justified by law, it must further be shown that the law under which the violation has taken place is just, fair and reasonable.

[76] The debate concerning data protection and data privacy in India started due to offshore outsourcing wherein personal data was exported by overseas companies to their off-shore agents or counterparts in India. If it was not for this mushrooming off-shoring business, India would perhaps never have worried much about data protection, as there are already existing provisions in the Indian legal framework for the protection of data privacy.

[77] NASSCOM, the coordinating body for India's software services industry, has established the self-regulatory Data Security Council of India (DSCI) in order to establish, monitor and enforce privacy and data protection standards for India's information technology and outsourcing industry.

[78] *See* CHARLES D. RAAB ET AL., APPLICATION OF A METHODOLOGY DESIGNED TO ASSESS THE ADEQUACY OF THE LEVEL OF PROTECTION OF INDIVIDUALS WITH REGARD TO PROCESSING PERSONAL DATA: TEST OF THE METHOD ON SEVERAL CATEGORIES OF TRANSFER (1998).

[79] The Information Technology Act, 2000 provides for civil liability in case of data theft, computer database theft, and privacy violation. Section 43 of the Act covers instances such as: (a) computer trespass, violation of privacy, etc.; (b) unauthorised digital copying, downloading and extraction of data, computer database or information and theft of data held or stored in any media; (c) unauthorised transmission of data or programme residing within a computer,

seems to have largely neglected the issue of privacy of personally identifiable information. However, there are other statutes which provide some safeguards to the lack of explicit legislation.[80] The Recovery of Debts Due to Banks and Financial Institutions Act, 1993, No. 51 of 1993, codifies India's tradition of maintaining confidentiality in bank transactions. Privacy in telecommunications is regulated by the Telecom Regulatory Authority of India (TRAI). The Common Charter of Telecom Services for adoption by all Telecom Service providers stipulates that "all Service Providers assure that the privacy of their subscribers (not affecting the national security) shall be scrupulously guarded."[81] Additionally, according to the Credit Information Companies (Regulation) Act, 2005, No. 30 of 2005, credit information pertaining to individuals in India has to be collected as per privacy norms enunciated in the applicable regulations.[82] Certain older laws are also relevant. The Indian Contract Act, 1872, No. 9 of 1872, offers an alternative solution to protect data as Indian companies acting as 'data importers' may enter into contracts with 'data exporters' to adhere to a high standard of data protection. The Specific Relief Act, 1963, No. 47 of 1963, provides preventive relief in the form of temporary and perpetual injunctions in order to prevent the breach of an existent obligation, whether expressly or by implication. However, the outcomes, though, depend on judicial interpretation. The Indian Telegraph Act, 1885, No. 13 of 1885, recognises privacy as a right but the government has the power to intercept communication for national security.

Although the Information Technology Act, 2000 attempts to address the issue of protecting privacy rights, it fails to meet the breadth and depth of protection that the E.C. Directive mandates[83] as it only protects privacy rights from government action. It is unclear whether such protection extends to private actions. Furthermore, unlike the E.C. Directive which imposes liability on each participant within the chain of command of the data who failed to protect the sanctity of the data, existing Indian laws only prosecute those individuals who directly violate laws

---

computer system or computer network (cookies, spyware, GUID or digital profiling are not legally permissible); (d) data loss, data corruption, etc.; (e) computer data or computer database disruption, spamming, etc.; (f) denial of service attacks, data theft, fraud, forgery, etc.; (g) unauthorised access to computer data or computer databases; and (h) instances of data theft.

[80] A few of these laws are section 65, section 66 and section 72 of the Information Technology Act, 2000, No. 21 of 2000, the Indian Contract Act, 1872, No. 9 of 1872, section 406 and section 420 of the INDIA PEN. CODE, 1860, No. 45 of 1860, and the Indian Copyright Act, 1957, No. 14 of 1957.

[81] *See* TELECOM REGULATORY AUTHORITY OF INDIA – COMMON CHARTER OF TELECOM SERVICES (2005), *available at* http://www.trai.gov.in/citizencharter/comm_charter16mar2006.pdf.

[82] It is my understanding that companies collecting and storing the data have been made liable for suspected leak or alteration of this data.

[83] § 43(b) of the Information Technology Act, 2000 is limited in scope.

related to computer systems.[84] Companies or individuals are exempted from liability for breaches of data privacy unless such violations were made knowingly.[85] Moreover, unlike the E.C. Directive which protects against data breaches by limiting data collection and use, the Indian laws do not specify conditions under which data can be collected and used.[86]

The Information Technology Act, 2000 has introduced some form of control over the use of encryption for communication in India.[87] The viability of this provision, however, remains questionable although the right to an encrypted transmission may be viewed as integral to the right to privacy flowing from Article 21 of the Constitution. The right can only be curbed by a 'procedure established by law.' As discussed before it is now well settled that such a procedure must be right, just, fair and reasonable to be valid. Whether the procedure under section 69 is sufficient to thwart the right to privacy remains to be tested.

It had become increasingly evident that the Information Technology Act, 2000 did not have suitable privacy and data protection provisions, and so the Indian government had appointed an Expert Committee on Cyber Laws whose role was to suggest amendments. The Committee proposed the following: (i) a new section 43(2) relating to the handling of sensitive personal data or information with reasonable security practices and procedures thereto; (ii) gradation of severity of computer related offences under section 66, committed dishonestly or fraudulently and punishment thereof; (iii) fine-tuning of section 72(1); (iv) additional section 72(2) in relation to breach of confidentiality with intent to cause injury to a subscriber; (v) language of section 66 pertaining to computer related offences to be revised in order to be in line with section 43 related

[84] § 43(b) of the Information Technology Act, 2000 only provides desultory safeguards against breaches in data protection. The scope of section 43(b) is limited to the unauthorized downloading, copying or extraction of data from a computer system, essentially unauthorized access and theft of data from computer systems. Section 43(b) is limited in scope, and so fails to meet the breadth and depth of protection that the E.U. Directive mandates.

[85] § 79 of the Information Technology Act, 2000, No. 21 of 2000.

[86] The E.C. Directive mandates five principles in accordance with which data must be collected and processed, including the requirement that the collection of data must be specific to the purpose for which it is collected, and such purpose must be disclosed to the data subject. It is based on a set of data protection principles, which include the legitimate basis, purpose limitation, data quality, proportionality, and transparency principles, data security and confidentiality, data subjects' rights of access, rectification, deletion and objection, restrictions on onwards transfers, additional protection where special categories of data and direct marketing are involved, and a prohibition on automated individual decisions. The E.C. Directive also requires that data must be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. *See* Council Directive 1995/46, 1995 O.J. (L 281) 31 (EC).

[87] § 69 of the Information Technology Act, 2000, No. 21 of 2000. It provides the Controller of Certifying Authorities with the power to intercept any transmission if certain criteria are satisfied and one such criterion provided for is the security of the state and concerns about the sovereignty and integrity of the nation.

to the penalty for damage to computer resources.[88] The Information Technology Amendment Act, 2008, No. 10 of 2009[89] was enacted to set the ball rolling in addressing the lacuna of data protection laws in the country through Sections 43A[90] and 72A.

The Information Technology Act, 2000 (as amended) now requires companies to maintain reasonable security practices, and procedures as to sensitive personal data or information, but does not define the phrase 'reasonable security practices and procedures.' As understood from the section 43A, reasonable security practices and procedures are to be determined as per the following manner: "as defined between the parties by mutual agreement or as specified in any law for the time being in force or to be specified by the Central Government in consultation with such professional bodies or associations as it may deem fit."[91] However, till date there is no law specifying reasonable security practices and procedures, nor has the Central government defined the security practices and procedures to be implemented in order to protect vital data. In the absence of such defined security practices and procedures, it is open for the parties to enter into agreements and lay down their own methods to protect their sensitive information and section 43A not only provides the freedom for doing so but also penalises any breach of such contractual obligations.

---

[88] CRID – UNIVERSITY OF NAMUR, FIRST ANALYSIS OF THE PERSONAL DATA PROTECTION LAW IN INDIA (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf. The offences have been graded according to the degree of severity of the offence when committed by any person, dishonestly or fraudulently without the permission of the owner. Keeping in line with the broad principles in E.C. Directive 2000/31/EC, section 79 has been revised to bring out explicitly the extent of the liability of the intermediaries in certain cases.

[89] The Lok Sabha (the Lower House of the Parliament of India) had hurriedly passed the Information Technology (Amendment) Bill, 2008 without even a debate as the discussion centred on political one-upmanship, rather than legislation. It received the assent of the President of India on 5th February 2009 and it came into force on 27th October 2009.

[90] Section 43A reads as follows: Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected. Explanation: For the purposes of this section (i) body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; (ii) reasonable security practices and procedures means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit; (iii) sensitive personal data or information means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[91] § 43A of the Information Technology Act, 2000, No. 21 of 2000.

Policy discourses in India have emphasised external forces as drivers of privacy policies. Hence of more significance is the Personal Data Protection Bill, 2006[92] drafted for the protection of personal data and information of an individual collected for a specific purpose and to prevent its usage by other organisations for commercial or other purposes. The draft Bill states that the personal data of any person collected for "a particular purpose or; obtained in connection with any transaction, whether by appropriate Government or by any private organization, shall not be put to processing; without the consent of the person concerned."[93] This straightforward approach is to be commended; however it does get distracted from the diversity of culture to which this could be applied since, as noted earlier, the Indian conception of privacy, being rooted in the local culture, is rather different from the West. Even the E.U.'s Assessment of Adequacy Report acknowledged the effect of differing political and cultural values on the interpretations of standards of 'adequacy' of data privacy protection measures to meet the E.U. standards. A final difficulty is that of cultural and institutional non-equivalence. Hence, all judgments about adequate protection must remain sensitive to important cultural differences.

Over the years, conflicts over data protection standards have led to several major international efforts aimed at the harmonization of information privacy standards.[94] However, despite the growing convergence of international data protection policy, 'privacy' still means something very different in various cultural and national traditions, perhaps particularly in non-Western jurisdictions but by no means there alone.[95] There are more important issues especially in terms of making information users aware of the issues involved. Stringent norms of protection and security are unlikely to quickly transform the existing norms of privacy in the interplay of private and public realms in India. The benefits of homogeneity must be balanced with the rights of legitimate authorities to determine laws within their jurisdictions. Finally, the seminal issue that remains

---

[92] The Personal Data Protection Bill, 2006 which was presented in the Rajya Sabha (the Upper House of the Parliament of India) in 2006, is still to be passed. It is highly unlikely that it will be passed in next 12 months.

[93] The Personal Data Protection Bill, 2006 requires that every organisation, whether it be governmental or private, engaged in the commercial transaction and collection of the personal data of persons shall – report to the Data Controller the type of personal data and information being collected and the purpose for which it is being or proposed to be used; take adequate measures to maintain confidentiality and security in the handling of personal data and information; and collect only such information that is essential for completion of any transaction with the individual. In order to give effect to the provisions of this scheme, the Central government can make further provisions so long as they are not inconsistent with the existing provisions.

[94] *See* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANS-BORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[95] *Supra* note 78, at 202.

even if the laws are in place is that it will still be required to be enforced in such manner as to provide any meaningful protection.

VI

CONCLUSION: INVENTING THE RIGHT WAY

The purpose of this paper has been to highlight the unjustified scaremongering of Western popular press which often portrays India in negative light when it comes to the protection of privacy. So should India think about reforming the law or could the issue be just about re-educating the people? Experience and evidence suggest that India should not take any deranged measures and should conduct an assessment of the necessity of the measure in question and its suitability for achieving its objective and the consequent balancing of the resulting restrictions. It should evaluate the options for general regulatory, legislative, self-regulatory and voluntary steps that can enhance privacy in order to ensure effectiveness. I would not deny that the creation of legal regulations are not always driven by practical needs; often it is driven by political aspirations and most of the time because of economic needs where dominant interest groups seek rules that allow markets to function more effectively. In my opinion, a key argument in favour of regulation is that it may be a more effective form of commitment than contractual arrangements. Gerety argues that the problem for the concept of privacy "comes not from the concept's meagreness but from its amplitude, for it has a protean capacity to be all things to all lawyers. A legal concept will do us little good if it expands like a gas to fill up the available space."[96] There can never be a purely legislative solution to privacy, neither there can be a 'model' legislative framework as socio-economic issues are unique to countries and have be considered in their own right for alleviating concerns over privacy. India could develop a new model, a model that is particularly Indian.

The independent existence of the right to privacy, as emerging from the customs and traditions of the people in addition to being a statutory right, must be recognised. I do not agree that 'umbrella' data privacy legislation similar to the E.U. Directive should ever be enacted by India, particularly when the E.U. Directive in itself is seen as a serious obstacle to global commerce and e-commerce. I also argue that it is also not the first time that different countries have responded differently to legal issues arising due to a technological development. Over the last decade or so, an increasing amount of studies point out how countries have varying routines in addressing public problems, in conducting public debates, in making public policies and in evaluating 'evidence' brought forward

[96] Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 234 (1977).

in the context of such problems.[97] Since inception, the E.U. Directive has been severely criticised. However, it is thriving because of the conceptual vacuum surrounding the legal notions of privacy. Bergkamp also questions the often presumed desirability and necessity of the E.U. Directive.[98] Although, the E.U. data protection regime was conceived as a linear, single-issue scheme, it became paradoxical and has had several unintended adverse effects. According to the E.U. Directive, the notion of personal data is very wide so as to cover all information which may be linked to an individual. However, there are no necessarily sufficient safeguards to ensure that data does not become personal data when it is not intended to be as such. The E.U. Directive represents one of the most restrictive data privacy laws in existence on the planet; it imposes an onerous set of requirements on any person who collects or processes data pertaining to individuals in their personal or professional capacity. It is argued that the restrictive approach of the E.U. towards data privacy laws is justified as it espouses the protection afforded by E.U. law. However, this approach is criticised by multinational organisations on the grounds that it creates an intolerable global trading environment and also because it hampers free trade. Indeed, it is remarkable that governments have been able to adopt and implement such an onerous, expensive and paradoxical data protection regime without any plausible evidence of harm or threatened harm, entirely based on some vague notion of a 'fundamental right' and hypothetical risks. In its rhetoric, the E.U. has misled the public to believe that its data protection regime was merely an implementation of pre-existing fundamental rights. Where law is an appropriate and effective instrument, there is a need to identify the harm with precision so that a precise and targeted solution is arrived at that does not cause 'collateral damage.' If we want to achieve global privacy standards, the E.U. will have to demonstrate greater respect for other countries' approaches to privacy regimes.

In a pluralistic society where democratic traditions require compromise and consensus, the obvious solution I strongly recommend is a balancing framework based on a realistic set of standards that weighs the benefits of the free flow of information against the possible threats to privacy on a case-by-case basis. My argument fits well with Dworkin's theory of law[99] which supports the balancing of interests when the quest is for a single right answer and also favours the utilitarian approach of relying upon the consequences of actions. As I have mentioned before in this paper, there are several examples of Indian companies acting as 'data importers' entering into

---

[97] *See* SHEILA JASANOFF, DESIGNS ON NATURE: SCIENCE AND DEMOCRACY IN EUROPE AND THE UNITED STATES (2005).

[98] Lucas Bergkamp, *The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER L. & SECURITY REP. 31 (2002).

[99] *See* Ronald Dworkin, *Hard Cases*, 88 HARV. L. REV. 1057 (1975).

contracts with 'data exporters' and also adhering to a high standard of data protection. These contracts are binding and fulfil the requirements of the overseas customers' national legislations.[100] A large number of Indian companies that are active in the information technology and outsourcing sectors at present have very stringent policies in relation to the protection of their clients' information and all employees are contractually bound to protect confidential information which may be processed.[101] The employment contracts clearly specify that the employees have to maintain as secret and confidential all such information which the company specifies from time to time. Many service providers in India have also engaged in voluntary self-regulation and adopted stringent security measures to reduce the risk of misuse of non-public personal data. Further, the establishment of the Data Security Council of India (DSCI) under the auspices of NASSCOM is definitely a positive step in the right direction. The objective of the DSCI is to create trustworthiness amongst Indian companies as global service providers by generating awareness of privacy and security issues. This re-emphasises my initial argument of not having the need to enact separate data privacy legislation modelled after the E.U. Directive.

I propose that the concept of privacy be imagined as a part of the 'collective good' which is important for the furtherance of 'social good,' thus leaving it open to us to adopt a broader concept of privacy and to determine how extensively it ought to be protected. Ironically, this is conceptually quite different from the more 'individual' Western perception. It is absolutely imperative that these standards are aligned to today's commercial realities and political needs, but they must also reflect technological realities. The implications of this view are significant. Perhaps most basic is the assumed fact of human diversity, wherein, as Locke put it, "men may choose different things, and yet all choose right." The regulation of privacy cannot be focused just on legislation and in any event will soon prove too complex. The way forward would be to move from precarious and unwarranted data protection legislation to the creation of effective policies which are designed to change the public perception of privacy as it cannot be denied that those who possess or process private information should bear a duty of confidentiality with respect to its dissemination.

---

[100] For example, all of the contracts with US based companies contain terms and specific conditions in relation to data protection that are in line with the Gramm-Leach-Bliley Act of 1999 and the Health Insurance Portability and Accountability Act of 1996.

[101] NASSCOM has established the National Skills Registry (NSR), a database of verified employees that includes biometric details and allows employers to verify the staff that they are recruiting. The NSR currently has details in relation to around 100,000 employees.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 6, 2010

SUI GENERIS PROTECTION FOR PLANT VARIETIES AND TRADITIONAL KNOWLEDGE IN BIODIVERSITY AND AGRICULTURE: THE INTERNATIONAL FRAMEWORK AND NATIONAL APPROACHES IN THE PHILIPPINES AND INDIA

Christoph Antons[*]

ABSTRACT

The so-called 'biotechnology clause' of Article 27.3(b) of the WTO-TRIPS Agreement requires from member states protection for plant varieties either via the patent system or via an 'effective sui generis system' or by a combination of the two. Many developing countries prefer forms of sui generis protection, which allow them to include exceptions and protection measures for traditional agricultural practices and the traditional knowledge of farmers and local communities. However, 'traditional knowledge' remains a vaguely defined term. Its extension to biodiversity has brought a diffusion of the previously clearer link between protected subject matter, intellectual property and potential beneficiaries. The Philippine legislation attempts a 'bottom-up' approach focusing on the holistic perceptions of indigenous communities, whereas national economic interests thus far receive priority in India's more centralist approach. Administrative decentralisation, recognition of customary rights, disclosure requirements, registers of landraces and geographical indications are discussed as additional measures, but their implementation is equally challenging. The article concludes that many of the concepts remain contested and that governments have to balance the new commercial incentives with the biodiversity considerations that led to their introduction, so that the system can be made sufficiently attractive for both knowledge holders and potential users of the knowledge.

[*] Professor of Comparative Law; Director, Centre for Comparative Law and Development Studies in Asia and the Pacific; Research Associate, Centre for Asia-Pacific Social Transformation Studies (CAPSTRANS), University of Wollongong, Australia; Chief Investigator, ARC Centre of Excellence for Creative Industries and Innovation (CCI); Adjunct Research Fellow, Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich. E-mail: cantons@uow.edu.au.

TABLE OF CONTENTS

I

BACKGROUND

The legal protection of plant breeders in developed countries goes back to the 1920s and 1930s.[1] More recently, it has expanded dramatically with the various amendments of the UPOV Convention,[2] and also following the 'biotechnology revolution', which in turn led to a more liberal use of the principles of patent law for subject matter of a biological nature.[3] However, while the debate has advanced rapidly in the industrialised world, it is still relatively new to developing countries, whose intellectual property systems are still focused on the more conventional and established forms of intellectual property rights such as trademarks and copyright. As in so many other fields of intellectual property, the WTO-TRIPS Agreement accelerated the process of introducing intellectual property rights for plant material to developing countries. The so-called 'biotechnology clause' of Article 27.3(b) allows WTO member states to exclude plants and animals and essentially biological processes for the production of plants or animals from patenting, but it requires the availability of patents for micro-organisms and non-biological and microbiological processes. In addition, it requires protection for plant varieties, which member states may provide either via the patent system or via an 'effective *sui generis*' system or by using a combination of the two systems.[4]

Because of its potential impact on food security, traditional farming methods and the livelihood of small-scale farmers in developing countries, the provision has been among the most controversial aspects of the TRIPS Agreement. As a consequence, a provision was made for a review of Article 27.3(b) four years after the WTO Agreement came into force. However, this review process, which should have taken place in 1999, has been marred by difficulties and even by disagreement over the meaning of the term 'review.' Some developing countries have brought forward far-reaching proposals to amend Article 27.3(b). The thrust of such proposals is to prohibit patenting of life forms and to strengthen the traditional rights of farmers to the use of saved seeds (farmers' rights), traditional knowledge about plants and farming methods and the preservation of biological

---

[1] *See, e.g.*, the Plant Patent Act, 35 U.S.C. §§ 161-164 (1930).

[2] UPOV stands for the International Union for the Protection of New Varieties of Plants.

[3] For details, *see* LIONEL BENTLY & BRAD SHERMAN, INTELLECTUAL PROPERTY LAW (2003).

[4] For details, *see* Margaret Llewelyn, *Which Rules in World Trade Law – Patents or Plant Variety Protection*, *in* INTELLECTUAL PROPERTY: TRADE, COMPETITION AND SUSTAINABLE DEVELOPMENT 303-339 (Thomas Cottier & Petros C. Mavroidis eds., 2003).

diversity.[5] Developed country members of the WTO, on the other hand, have argued that any review of Article 27.3(b) should only concern the implementation of the provision. For developed country members with advanced biotechnology industries such as the US, the aim is rather to eliminate the exclusion from patentability of plants and animals and to restrict the freedom for developing countries to develop their own *sui generis* systems for plant variety protection by relying as far as possible on the UPOV Convention in its 1991 version.

Possible elements of such *sui generis* protection systems and their relationship to forms of traditional knowledge are the subject of this article. In view of the concerns of developing countries regarding patents in this field, many countries so far show a preference for *sui generis* protection for plant varieties to the patenting option or a blending of the two systems.

The article will begin with an explanation and an update of the international framework of the debate and of the terminology used for various forms of traditional knowledge, which is essential for an understanding of the national efforts that are undertaken in this field. It will then analyse UPOV as the "ready-made" solution to implement plant variety protection and discuss alternative models and additional provisions that provide practical solutions. Finally, it will provide two case studies of national approaches, that of the Philippines and India. The examples show quite different policy approaches, a more decentralised approach focusing on indigenous peoples in the Philippines and a more centralised approach to the administration of farmers' rights and access to biodiversity in India. Some of these differences are less accentuated if one examines the actual implementation of the policies. In addition, with the recently released Protection, Conservation and Effective Management of Traditional Knowledge Relating to Biological Diversity Rules of 2009, India also attempts to move to more decentralised mechanisms for access to traditional knowledge and benefit sharing. The Philippine experience indicates, however, that too stringent conditions may scare off potential applicants and that for the system to operate successfully, it is important to find the right balance between the interests of knowledge holders and the expectations of users seeking access.

[5] *See* UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD) & INTERNATIONAL CENTRE FOR TRADE AND SUSTAINABLE DEVELOPMENT (ICTSD), RESOURCE BOOK ON TRIPS AND DEVELOPMENT 396-397 (2005) (submission to the WTO Council by the African Group of Countries in 2003).

II

THE INTERNATIONAL FRAMEWORK FOR TRADITIONAL KNOWLEDGE, ACCESS TO GENETIC RESOURCES AND PLANT VARIETY PROTECTION

While the use of intellectual property law related to life forms expanded, particularly in industrially advanced countries, there has been a tightening of access to the biological resources necessary for biotechnological research in the most bio diverse countries of the world, which are predominantly developing countries. Thus, while the non-binding International Undertaking on Plant Genetic Resources of 1984 still regarded plant genetic resources as "heritage of mankind" and as freely accessible and exchangeable,[6] the 1992 Convention on Biological Diversity (CBD) gave nation states "the sovereign right to exploit their own resources pursuant to their own environmental policies" (Article 3, CBD) and provided that "the authority to determine access to genetic resources rests with the national governments and is subject to national legislation" (Article 15(1), CBD).[7] The CBD discourages neither biotechnological research (Article 19, CBD) nor intellectual property rights (Article 16(2), CBD). However, intellectual property rights should be "supportive of and not run counter to" the objectives of the CBD (Article 16(5)). Resource-rich parties are required to "endeavour to create conditions to facilitate access to genetic resources for environmentally sound uses" (Article 15(2), CBD), while technologically advanced users shall provide access to and transfer of technology relevant for or resulting from the sustainable use of genetic resources (Article 16, CBD) as well as participation in relevant research projects (Article 15(6), CBD). Access to such resources shall be on "mutually agreed terms" (Article 15(4), CBD) and with "prior informed consent" (Article 15(5), CBD) and shall lead to fair and equitable sharing of "the results of research and development and the benefits arising from the commercial and other utilization of genetic resources" (Article 15(6), CBD). Importantly, while the International Undertaking on Plant Genetic Resources and the subsequent Plant Genetic Resources Treaty are confined to plants for food and agriculture, the CBD extends also to plants for medicinal and pharmaceutical purposes. Indeed, desire by providing countries of genetic

---

[6] Michael Blakeney, *Intellectual Property Aspects of Traditional Agricultural Knowledge*, *in* IP IN BIODIVERSITY AND AGRICULTURE 44 (Peter Drahos & Michael Blakeney eds., 2001); Carlos Correa, *Access to Plant Genetic Resources and Intellectual Property Rights*, *in* IP IN BIODIVERSITY AND AGRICULTURE 105 (Peter Drahos & Michael Blakeney eds., 2001).

[7] The shift in the CBD was preceded by similar resolutions at the FAO conferences in 1989 and 1991 that added Annexes to the International Undertaking on Plant Genetic Resources. *See* Gregory Rose, *International Law of Sustainable Agriculture in the 21st Century: Resources for Food and Agriculture*, 15 GEO. INT'L ENVTL. L. REV. 583, 602 (2003).

resources to share in the profits made from pharmaceutical research was a substantial reason for the negotiation of Article 15.[8]

While the parties to the convention are of course nation states, the CBD foresees an important role for indigenous and local communities. According to Article 8(j) of the CBD, each party, subject to its national legislation, is required to "respect, preserve and maintain knowledge, innovations and practices of indigenous and local communities embodying traditional lifestyles relevant for the conservation and sustainable use of biological diversity and promote their wider application with the approval and involvement of the holders of such knowledge, innovations and practices and encourage the equitable sharing of the benefits arising from the utilization of such knowledge, innovations and practices." In other words, parties to the Convention are required to pass on the benefits of the Convention and to replicate benefit-sharing mechanisms at the local level.

The shift to national sovereignty over biological resources has been further reaffirmed in the International Treaty on Plant Genetic Resources for Food and Agriculture (ITPGRFA), negotiated under the auspices of the United Nations Food and Agriculture Organization (FAO). In creating a multilateral system of access and benefit sharing, the parties "recognize the sovereign rights of States over their own plant genetic resources for food and agriculture, including that the authority to determine access to those resources rests with national governments and is subject to national legislation" (Article 10, ITPGRFA). However, in contrast to the CBD, the ITPGRFA relates only to plant genetic resources for food and agriculture and the multilateral system covers essential food crops listed in Annex I of the Treaty. The Treaty promotes a standard material transfer agreement (MTA) with certain mandatory provisions,[9] including the limitation of access to food and agriculture related purposes of utilisation and conservation for research, breeding and training (Article 12.3(a), ITPGRFA), a prohibition for the recipients to claim intellectual property rights or other rights limiting facilitated access (Article 12.3(d), ITPGRFA), the continuous process of making available conserved resources by the recipients (Article 12.3(g), ITPGRFA) and the payment of an equitable share of the benefits arising from the commercialisation of products incorporating accessed materials to a Trust Account established by the Governing Body of the Treaty (Article 13.2(d)(ii), ITPGRFA). The last mentioned article also provides that the Governing

[8] *Id.* at 607.

[9] The predecessors of these MTAs are to be found in the agreements between the FAO and the International Agricultural Research Centres (IARCs) within the Consultative Group on International Agricultural Research (CGIAR). *See supra* note 7, at 595.

Body may decide to establish different levels of payment for various categories of recipients and may decide to exempt small farmers from developing countries or countries with economies in transition from such payments.

In contrast to the bilateral mechanisms thus far available under the CBD, the access and benefit sharing mechanism promoted by the ITPGRFA is a multilateral system. Since payments to the envisaged trust fund are not mandatory for material "available without restriction", payments are mandatory mainly for plant patent holders, but not necessarily for holders of plant breeders' rights.[10] Under the circumstances and given the absence of the main patenting nations US and Japan from the ITPGRFA[11], the available funds under the system will remain very small and are unlikely to even cover the administrative costs of the treaty.[12] And while the ITPGRFA still covers in its Annex approximately 80-90 per cent of the most vital crops, a number of vital crops were not included, because specific developing countries were not willing to add them to the list.[13]

Similar to the CBD and the earlier International Undertaking on Plant Genetic Resources, the ITPGRFA recognises the traditional knowledge of local and indigenous communities and of farmers in Article 9 on 'Farmers' Rights. ' In particular, it encourages national governments to realise farmers' rights by protecting and promoting traditional knowledge relevant to plant genetic resources for food and agriculture, the right to equitably participate in sharing benefits from the utilisation of plant genetic resources and the right to participate in decision making at the national level on the conservation and sustainable use of food and agriculture related plant genetic resources (Article 9.2, ITPGRFA). However, the treaty language is couched in the most qualified terms. Parties have to protect and promote farmers' rights "in accordance with their needs and priorities" and "as appropriate, and subject to national legislation." Article 9.3 of the treaty reserves the traditional farmers' privilege to "save, use, exchange and sell farm-saved seed/propagating material, subject to national law and as appropriate."

---

[10] *See* Charles R. McManis & Eul Soo Seo, *The Interface of Open Source and Proprietary Agricultural Innovation: Facilitated Access and Benefit-Sharing under the New FAO Treaty*, 30 WASH. U. J.L. & POL'Y 405, 452-453 (2009) (it is argued that UPOV-compliant plant variety protection as well as intellectual property rights with sufficiently broad 'experimental use' privileges will not 'limit facilitated access' under Article 12.3(d)).

[11] The United States signed the treaty in 2002, but did not move further to accession, approval, acceptance and ratification. *See* List of Contracting Parties, http://www.fao.org/Legal/treaties/033s-e.htm (last visited 6th July 2010).

[12] *See supra* note 10, at 460 (quoting a calculation by the NGO Berne Declaration that on the basis of an estimated seed market of $30 billion in 2019, income from benefit-sharing will be as little as $2.31 million per year.

[13] As for example with the inclusion of soybeans that was objected to by China. For this aspect of the debate and for further examples, *see supra* note 7, at 616. *See also supra* note 10, at 460 (provides further examples).

Of the various provisions of the treaty, the obligation not to claim "intellectual property or other rights that limit the facilitated access to the plant genetic resources for food and agriculture, or their genetic parts or components, in the form received from the Multilateral System" has been controversial. While the provision has been interpreted as not covering intellectual property rights to germplasm modified by the recipient,[14] the provision is regarded as one of the reasons for the absence from the treaty of both the US and Japan, the two main countries active in the patenting of life forms.

Since the Johannesburg World Summit on Sustainable Development in 2002, an international regime for access and benefit sharing is further being negotiated in the Ad Hoc Open-Ended Working Group on Access and Benefit-Sharing of the Convention on Biological Diversity. The latest meeting of the Working Group in Cali, Colombia, in March 2010 produced a revised Draft Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization. The Working Group hopes to finalise negotiations on the Draft Protocol in time for the next Conference of the Parties of the CBD in Nagoya, Japan, in October 2010.[15]

III

THE RELATIONSHIP BETWEEN PROTECTED SUBJECT MATTER, TRADITIONAL KNOWLEDGE, INTELLECTUAL PROPERTY RIGHTS AND THE BENEFICIARIES OF ANY FORM OF PROTECTION

The term "traditional knowledge" is used in the international debate in various forms, with often widely diverging coverage of subject material, different elements of the intellectual property system and with different stakeholders and beneficiaries, the interests of whom do not always coincide. It is, therefore, necessary at the outset to gain some understanding of the meaning of the term for the purposes of this article.[16] A widely used first working definition stemmed from a WIPO study of

---

[14] Michael Blakeney, *Bioprospecting and Biopiracy*, *in* INTELLECTUAL PROPERTY AND BIOLOGICAL RESOURCES 393, 417 (Burton Ong ed., 2004). The interpretation hinges on the term 'in the form received' which was one of the most contentious issues during the treaty negotiations, *see supra* note 10, at 453.

[15] Conference of the Parties to the CBD, Ad Hoc Open-ended Working Group on Access and Benefit-Sharing, *Report of the First Part of the Ninth Meeting of the Ad Hoc Open-ended Working Group on Access and Benefit-Sharing*, U.N. Doc. UNEP/CBD/WG-ABS/9/3 (Apr. 26, 2010), *available at* http://www.cbd.int/doc/meetings/abs/abswg-09/official/abswg-09-03-en.pdf.

[16] Whether at least 'broad, non-exhaustive and non-exclusive definitions' are necessary or whether a more loosely worded terminology is sufficient remains contested. As for traditional cultural expressions, *see* Christoph Antons, *What is 'Traditional Cultural Expression?' – International Definitions and their Application in Developing Asia*, 1 WIPO J. 103, 104 (2009) (the statements of the representatives of New Zealand and Singapore, on the one hand, and of Nigeria, on the other hand).

2001[17] on the needs and expectations of traditional knowledge holders, which in turn was based on fact-finding missions to various parts of the world undertaken in 1998 and 1999. 'Traditional knowledge' according to this working definition comprised "tradition-based literary, artistic or scientific works; performances; inventions; scientific discoveries; designs; marks, names and symbols; undisclosed information; and all other tradition-based innovations and creations resulting from intellectual activity in the industrial, scientific, literary or artistic fields." This working definition was clearly influenced by a more holistic understanding of traditional knowledge as encompassing forms of art as well as knowledge about the healing effects of plants and about the environment. This understanding is particularly common among many indigenous societies, which are not using elaborate writing systems to transmit their knowledge. Here, art forms such as songs, stories, dances and paintings are frequently used to collectively memorise the knowledge and to transmit it to following generations. As a result, cultural expressions and objects and their included traditional knowledge acquire a secret and sacred status in some indigenous societies[18] that makes it difficult to distinguish between artistic expressions and scientifically relevant knowledge in the way that intellectual property lawyers are familiar with.[19]

That the character of the holders of the knowledge and the culture and forms of life of the community are important in defining traditional knowledge follows from a further clarification from the WIPO report. Accordingly, "tradition-based refers to knowledge systems, creations, innovations and cultural expressions which: have generally been transmitted from generation to generation; are generally regarded as pertaining to a particular people or its territory; and are constantly evolving in response to a changing environment." Since the knowledge pertains to a particular people or its territory, there is, therefore, a crucial link between the knowledge and its particular holder(s) that is very different from the neutral forms of ownership in other areas of

---

[17] World Intellectual Prop. Org. [WIPO], *Intellectual Property Needs and Expectations of Traditional Knowledge Holders: WIPO Report on Fact-finding Missions on Intellectual Property and Traditional Knowledge (1998-1999)* (April 2001), *available at* http://www.wipo.int/tk/en/tk/ffm/report/index.html (follow links 'Part 1' + 'Part 2' + 'Annex').

[18] Jurg Wassmann, *The Politics of Religious Secrecy*, *in* EMPLACED MYTH: SPACE, NARRATIVE AND KNOWLEDGE IN ABORIGINAL AUSTRALIA AND PAPUA NEW GUINEA (Alan Rumsey & James F. Weiner eds., 2001); Eric Kline Silverman, *From Totemic Space to Cyberspace: Transformations in Sepik River and Aboriginal Australian Myth, Knowledge, and Art*, *in* EMPLACED MYTH: SPACE, NARRATIVE AND KNOWLEDGE IN ABORIGINAL AUSTRALIA AND PAPUA NEW GUINEA (Alan Rumsey & James F. Weiner eds., 2001).

[19] Darell A. Posey, *Can Cultural Rights Protect Traditional Cultural Knowledge and Biodiversity?*, *in* CULTURAL RIGHTS AND WRONGS 43 (Halina Niec ed., 1998); Christoph Antons, *Traditional Cultural Expressions and Their Significance for Development in a Digital Environment: Examples from Australia and Southeast Asia*, *in* INTELLECTUAL PROPERTY AND TRADITIONAL CULTURAL EXPRESSIONS IN A DIGITAL ENVIRONMENT 288 (Christoph Beat Graber & Mira Burri-Nenova eds., 2008); Christoph Antons, *Traditional Knowledge in Asia: Global Agendas and Local Subjects*, *in* REGULATION IN ASIA: PUSHING BACK ON GLOBALIZATION 66 (John Gillespie & Randall Peerenboom eds., 2009).

intellectual property law. Identifying the holders of traditional knowledge becomes not just a practical necessity for the purposes of obtaining consent and for implementing forms of benefit sharing, but it also defines the "traditional" character of the subject matter. In other words, whether a certain form of knowledge is regarded as "traditional" will depend on the lifestyle, customary laws and forms of transmission used by its "owner" or "holder."[20]

Prior to any discussion about traditional knowledge in the context of biological diversity, farming practices and knowledge about the environment, the area of concern was largely "folklore", i.e., the protection of traditional forms of art and cultural expressions. This discussion goes back to the 1960s, when developing countries began to realise that their folkloristic material, in particular in the form of music, was being popularised and commercially exploited by companies from the industrialised world.[21] At the time, the discussion produced WIPO and UNESCO-sponsored model provisions for the protection of folklore and the Tunis Model Law for the Protection of Folklore of 1976. The first extension of the concept of traditional knowledge came with the emergence of the concept of farmers' rights in FAO Resolution 4/89. They were further defined in FAO Resolution 5/89 as "Rights arising from the past, present and future contribution of farmers in conserving, improving and making available Plant Genetic Resources, particularly those in the centres of origin/diversity. These rights are vested in the International Community, as trustees for present and future generations of farmers, for the purpose of ensuring full benefits of farmers and supporting the continuation of their contributions…".[22] With the arrival of the Convention on Biological Diversity, the concept of traditional knowledge was again further extended to include the "knowledge, innovations and practices of indigenous and local communities embodying traditional lifestyles relevant for the conservation and sustainable use of biological diversity."[23]

The CBD promoted the now widely required forms of benefit-sharing and prior informed consent as ethically important pre-conditions for the use of traditional knowledge. Of equal importance was, however, the fact that the Convention broadened the perspective from folklore to traditional knowledge and its impact on biodiversity and the environment. As far as plant material was concerned, the focus was now no longer only on agricultural foodstuff and the relatively settled

---

[20] *See also* WIPO, INTELLECTUAL PROPERTY AND TRADITIONAL KNOWLEDGE (FREE INFORMATION PRODUCT – BOOKLET NO. 2), *available at* http://www.wipo.int/freepublications/en/tk/920/wipo_pub_920.pdf.

[21] Michael Halewood, *Indigenous and Local Knowledge in International Law: A Preface to Sui Generis Intellectual Property Protection*, 44 MCGILL L.J. 953, 967-968 (1999).

[22] *See* Carlos Correa, *Options for the Implementation of Farmers' Rights at the National Level* 4 (S. Ctr., T.R.A.D.E. Working Paper No. 8, 2000).

[23] Convention on Biological Diversity art. 8(j), June 5, 1992, 1760 U.N.T.S. 79.

communities of traditional farmers and plant breeders. Biodiversity meant broadening the focus of the protected subject matter to plants related to, for example, forestry or pharmaceutical use[24] and to the people involved in their conservation and development, often forest dwellers and nomadic people, in many countries termed 'indigenous' because of their longer relationship with the land in comparison to a mainstream population that had arrived in later waves of migration.

However, while such knowledge may be held by people identifiable as indigenous, this is by no means a necessity. Just as folkloristic material may be provided by indigenous communities as well as by local non-indigenous communities inhabiting particular parts of a country, traditional knowledge about plants or the environment can now be held by indigenous people or by traditional healers or by farmers using traditional methods of farming particularly well suited to the local environment. Plants used in traditional medicines, for example, are sourced from forests as well as from private herbal gardens and, with increasing commercialisation of such medicines, also from commercial farms.[25] Anthropologists have further pointed out that the previous distinction between lowland farmers and forest conserving tribal people in the uplands in countries such as Thailand can no longer been maintained. While farmers have long begun to supplement their income with additional swidden agriculture in areas formerly regarded as tribal domains, tribal people have equally become agricultural labourers on farms outside of their tribal territories.[26] Thus, with the widening of the scope of potential holders of traditional knowledge, the focus has to some extent moved away from locally confined living communities (which to some degree has always been a legal fiction as people, including 'indigenous' people, are of course mobile) to the nation state. Traditional knowledge about farming or healing (arguably both forms of 'sustainable use') may well be held throughout a particular country and may be incorporated into national culture. Examples include Chinese traditional medicine, Indian ayurvedic medicine or Thai traditional medicine.

Thus, the extension of traditional knowledge to biodiversity in the CBD has brought a diffusion of the previously clearer (although by no means easily to establish) link between protected subject matter, intellectual property involved and the potential beneficiaries. Protectable subject matter

---

[24] *Supra* note 10. As McManis and Seo point out, approximately half of the world's medicines are estimated to contain compounds of plant origin.

[25] Christoph Antons & Rosy Antons-Sutanto, *Traditional Medicine and Intellectual Property Rights: A Case Study of the Indonesian Jamu Industry*, *in* TRADITIONAL KNOWLEDGE, TRADITIONAL CULTURAL EXPRESSIONS AND INTELLECTUAL PROPERTY LAW IN THE ASIA-PACIFIC REGION 363, 365 & 369 (Christoph Antons ed., 2009).

[26] TIM FORSYTH & ANDREW WALKER, FOREST GUARDIANS, FOREST DESTROYERS: THE POLITICS OF ENVIRONMENTAL KNOWLEDGE IN NORTHERN THAILAND 60-63 & 222 (2008).

comes in the form of knowledge and innovations relevant for the conservation and sustainable use of biological diversity. As outlined previously, this may be anything from the knowledge of forest dwellers or farmers about their environment or healing plants or local breeding conditions to nation-wide practised forms of traditional medicine using herbs and plants. The identification of potential right holders and beneficiaries has become equally difficult with their being defined now as "indigenous and local communities embodying traditional lifestyles." Finally, the focus on indigenous communities that often have no written tradition of transmitting their knowledge, has also meant that the previously clearer distinction between subject matter related to copyright (folklore) and other forms of traditional knowledge (agricultural plants and biodiversity) has become problematic in some countries. The use of artistic expressions for the transmission of knowledge by many of these people means that traditional knowledge from this perspective can now concern almost any form of intellectual property.

Folklore and farmers' rights have been widely accepted as concepts, although attempts at implementation have been uneven and often half-hearted and terms such as 'folk' art have occasionally been criticised as prejudicial, patronizing and outmoded.[27] However, the further extended form of traditional knowledge leading to some form of "intellectual property in biodiversity" is for many parties even more difficult to accept or to put into practice. It requires first of all the recognition that even plants grown in the wild are not really wild but have been modified by human impact, for example, through the deliberate use of fire for cultivation and regeneration purposes in rainforest areas and through slash and burn agricultural practices by indigenous and nomadic or semi-nomadic people. In other words, it requires a rehabilitation of the knowledge and practices of such forest dwellers, which thus far has been often blamed in official discourses for the destruction of forests.[28] It requires, secondly, the recognition of indigenous and local communities by the national government as groups that are able to hold rights separate from the mainstream population.

These requirements put many governments in developing countries into a difficult position. On the one hand, they appreciate the potential value of traditional knowledge, which can be used as a bargaining tool in negotiations with the industrialised countries. On the other hand, young nation states regard the promotion of a national identity as important. In countries that are still struggling

[27] Nelson H. H. Graburn, *Arts of the Fourth World*, *in* THE ANTHROPOLOGY OF ART: A READER 412, 413-414 (Howard Morphy & Morgan Perkins eds., 2006).

[28] For the historical background of such policies, *see* Nancy Lee Peluso & Peter Vandergeest, *Genealogies of the Political Forest and Customary Rights in Indonesia, Malaysia and Thailand*, 60 J. ASIAN STUD. 761 (2001).

to overcome thinking in tribal or community terms and focus instead on considerations at a national level, it is difficult to recognise the preferential interests of local or indigenous communities that the CBD requires. What's more, many national governments in fact blame 'backward' looking communities for the destruction of the rainforest and of biodiversity through slash and burn practices and shifting agriculture.[29] The difficulties in adopting an unequivocal position on traditional knowledge under these circumstances become visible from the examples in Asia presented at the end of this study. They are also becoming visible from the deliberations at WIPO regarding the creation of a voluntary fund to enable accredited and indigenous communities to participate in the debate of the Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge and Folklore. The governments of India and Indonesia in particular expressed concern about the use of the terms 'indigenous and local communities' and the exclusion of civil society at large that this implied. The Indonesian delegation expressed a preference for terms such as 'traditional society' or 'society or community bound by customary law.'[30] Equally, while voting in favour of the UN Declaration on the Rights of Indigenous Peoples in 2007, the Indonesian representative proceeded on the basis of ILO Convention No. 107 of 1957 "according to which indigenous people were distinct from tribal people" and concluded that "the rights in the declaration accorded exclusively to indigenous people and did not apply in the context of Indonesia."[31]

Perhaps recognising the difficulties in adopting a too extended definition, WIPO has in recent years moved back to an approach that distinguishes folklore/cultural expressions and what is now termed "traditional knowledge in the strict sense." In more recent publications, WIPO still acknowledges the holistic understanding and interrelationship between folklore and traditional knowledge (TK), but it maintains that the protection of traditional cultural expressions (TCEs)/folklore "is in practice distinct from but related to" the protection of TK. It was, therefore, necessary, to produce a second publication focusing on "the complementary protection of TCEs"

---

[29] For a critical assessment of such government positions, *see* CIVILIZING THE MARGINS: SOUTHEAST ASIAN GOVERNMENT POLICIES FOR THE DEVELOPMENT OF MINORITIES (Christopher R. Duncan ed., 2004).

[30] WIPO Secretariat, *Second Draft Report on Eighth Session of the Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge and Folklore*, 26-27, WIPO/GRTKF/IC/8/15 Prov 2 (Oct. 5, 2005), *available at* http://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_8/wipo_grtkf_ic_8_15_prov_2.pdf (for the Indian position, *see* 30, 40 & 48).

[31] *See* Press Release, U.N. General Assembly, General Assembly Adopts Declaration on Rights of Indigenous Peoples; 'Major Step Forward' Towards Human Rights for All, Says President (Sept. 13, 2007), *available at* http://www.un.org/News/Press/docs/2007/ga10612.doc.htm (statement of the Indonesian representative in the United Nations General Assembly).

whereas the TK publication was to focus "on the protection of TK as such – that is to say, the content or substance of knowledge."[32]

As a consequence, WIPO has produced separate draft model provisions for TCEs/folklore and for TK. In a reproduction of its document 'The Protection of Traditional Knowledge: Revised Objectives and Principles', WIPO defines the scope of the subject matter in Article 3(2) differently and in a manner that takes into account criticisms of earlier working definitions. Accordingly, traditional knowledge comprises:

> The content or substance of knowledge resulting from intellectual activity in a traditional context, and includes the know-how, skills, innovations, practices and learning that form part of traditional knowledge systems, and knowledge embodying traditional lifestyles of indigenous and local communities, or contained in codified knowledge systems passed between generations. It is not limited to any technical field, and may include agricultural, environmental and medicinal knowledge, and knowledge associated with genetic resources.[33]

While some countries have adopted the holistic approach expressed in the earlier WIPO working definition,[34] this article is predominantly concerned with the relationship between *sui generis* protection for plant varieties and traditional knowledge protection and therefore does not cover cultural expressions. The remaining forms of traditional knowledge protection and access legislation related to plant varieties are more difficult to separate, however, and only a few of the aims for various benefit-sharing mechanisms and encouragement of biodiversity protection can be realised via *sui generis* legislation for plant varieties. The following part of this article will begin by explaining the concept of farmers' rights. Agriculture is an area of traditional knowledge protection in which the identification of the traditional knowledge holders (and their reward or compensation) has been regarded as comparatively easier than in some of the other areas. In most developing countries, traditional knowledge holders are seen as largely identical with local farmers (indigenous or non-indigenous), as long as they are still practising some form of traditional

---

[32] *Supra* note 20.

[33] WIPO Secretariat, *Reproduction of Document WIPO/GRTKF/IC/9/5 "The Protection of Traditional Knowledge: Revised Objectives and Principles"*, WIPO/GRTKF/IC/12/5(c) (Dec. 6, 2007), *available at* http://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_12/wipo_grtkf_ic_12_5_c.pdf.

[34] *See, e.g.*, in the Philippines, An Act to Recognize, Protect and Promote the Rights of Indigenous Cultural Communities/Indigenous People, Creating a National Commission of Indigenous People, Establishing Implementing Mechanisms, Appropriating Funds Therefore, and for Other Purposes, Rep. Act 8371 (1997) (Phil.); *see also* Rule 2 (v) of the Protection, Conservation and Effective Management of Traditional Knowledge Relating to Biological Diversity Rules, 2009 (rules drafted by the National Biodiversity Authority of India; the definition of 'traditional knowledge' includes in the concept a list of cultural expressions).

farming.[35] The matter may become more controversial again, however, where it concerns forms of swidden agriculture. As was explained above, governments tend to regard such forms of agriculture as harmful to the environment.

IV

THE CONCEPT OF FARMERS' RIGHTS

It has often been said that the concept of Farmers' Rights is based on equity considerations to compensate traditional farmers for their past contributions in improving and making available Plant Genetic Resources for Food and Agriculture (PGRFA). While the concept had already been introduced in FAO discussions in the early 1980s and is now well established, the debate has recently turned to the question of how to best implement farmers' rights. Here, a market based solution, that is treating Traditional Plant Genetic Resources for Food and Agriculture (TPGRFA) as private goods is often contrasted with a compensation solution, in which TPGRFA remain in the public domain, but the nation states where they occur are empowered to negotiate compensation for their traditional farming sectors. Because of the difficulties in assessing the value of landraces and other forms of TPGRFA, the focus in this field has been on compensation approaches based on equity considerations, so that the use of 'rights' in this context has been largely symbolic. This means also that the paradigm shift from 'heritage of mankind' to proprietary concepts has been incomplete. While resources are now under national control, this control has not yet been further devolved to local communities, cooperatives or individuals. Further, the Multilateral System of the ITPGRFA, designed to counter the emerging proprietary concepts in this field, has been described as "a hybrid approach to agricultural innovation, combining open source and proprietary elements."[36]

V

ESSENTIAL AND FACULTATIVE ELEMENTS OF A *SUI GENERIS* SYSTEM FOR PLANT VARIETIES

As the WTO-TRIPS Agreement does not make reference to the UPOV Convention, the UPOV Acts of both 1978 and 1991 are suitable models for a national *sui generis* system. However, if a country wants to join UPOV as such, it must adopt the 1991 version, as the deadline for UPOV

---

[35] *See, e.g.,* Daniel Alker & Franz Heidhues, *Farmers' Rights and Intellectual Property Rights – Reconciling Conflicting Concepts* 14-15 (Inst. of Agric. Econ. and Soc. Sci. in the Tropics and Subtropics, Discussion Paper No. 2/2002, 2002), *available at* https://entwicklungspolitik.uni-hohenheim.de/uploads/media/DP_02_2002_Alker.pdf.

[36] *Supra* note 10, at 456.

members to join the 1978 Act was 24 April 1999.[37] Whether a country wants to join UPOV or adopt any of its Acts ultimately depends on its capacity and national ambition in the field of plant breeding. Both Acts promote commercial plant breeding. Because of the protection criteria of distinctness, uniformity and stability (commonly referred to as the DUS criteria) they have been criticised for furthering the genetic uniformity of crops and, thereby, being ultimately harmful to biodiversity. Both Acts are adequate for a country that has ambitions and realistic hopes for its plant breeding industry in the near future. The more ambitious and better positioned countries may want to join UPOV directly and thus have to adopt the 1991 version of the Act. The 1991 version extends the rights of breeders in comparison to the 1978 version. The acts which require authorisation under UPOV 1991 include according to Article 14: production or reproduction, conditioning for the purposes of propagation, offering for sale, selling or other marketing, exporting, importing and stocking for the aforementioned purposes. This compares to the still relatively simple list of rights in Article 5 of UPOV 1978, which is to authorise the production for purposes of commercial marketing, the offering for sale and the marketing of the reproductive or vegetative propagating material, as such, of the variety.[38]

More importantly, under UPOV 1991, the rights of the breeder also extend to the harvested material obtained through the use of propagating material and of "essentially derived" varieties. This means, first of all, that the so-called 'farmers' privilege' of re-using harvested seed from protected varieties no longer applies automatically, but it must now be specifically implemented by a government concerned about traditional farming practices. It is, therefore, now regulated as an exemption to breeders' rights in Article 15 of the 1991 version. Secondly, commentators from developing countries[39] have expressed concern about the vague criterion of the "essentially derived variety", which they expect to be settled more often than not through agreement or litigation rather than examination, thereby favouring the stronger party.[40] Even among those countries with ambitions to establish a commercial plant breeding sector, the choice between the two UPOV versions is, therefore, one of graduation and levelling out of the advantages and disadvantages. Countries with strong prospects for a commercial plant breeding sector may opt for direct

---

[37] TSHIMANGA KONGOLO, UNSETTLED INTERNATIONAL INTELLECTUAL PROPERTY ISSUES 64 (2008).

[38] For a comparison of the 1978 and 1991 versions of UPOV, *see* GRAHAM DUTFIELD, INTELLECTUAL PROPERTY RIGHTS, TRADE AND BIODIVERSITY 26-29 (2000).

[39] *See* Biswajit Dhar & Sachin Chaturvedi, *Introducing Plant Breeders' Rights in India – A Critical Evaluation of the Proposed Legislation*, 1 J. WORLD INTELL. PROP. 245 (2005).

[40] *Supra* note 10, at 424. McManis and Seo argue that the requirement that an essentially derived variety must be 'predominantly derived' from a protected variety and the examples of how an essentially derived variety can be obtained makes the scope of protection narrower than the one that copyright provides for 'derivative works.'

accession to UPOV and adoption of the 1991 version.[41] The majority of the developing countries in Asia will probably be fairly advanced in classical scientific breeding with a strong involvement of the public sector. Adoption of one of the UPOV versions seems a possibility here, perhaps in some cases modified along the lines of the various options outlined below.

For countries below that threshold, especially those with a mainly traditional farming sector and without any immediate prospects for a successful commercial plant breeding sector, modifications to the UPOV framework may be advisable. Leskien and Flitner have summarised options for such modifications in a report for the International Plant Genetic Resource Institute (IPGRI) of 1997.[42] First, countries may define the subject matter of protection more widely in their own interest. A wider definition of 'plant varieties', for example, would create space for the recognition of 'traditional' or 'local varieties', which are not as uniform as varieties under the UPOV definition and could be distinguished from these commercial varieties. Moreover, there is nothing in the TRIPS Agreement preventing countries from extending the protection of a *sui generis* legislation to traditional knowledge and farmers' rights.[43] Second, TRIPS allows for variation of the so-called DUS requirements of UPOV (referring to the necessity for protection that a plant variety must be distinct, uniform and stable). While distinctness is a requirement also under TRIPS, the wording used should make it plain that more than merely 'cosmetic breeding' is required. But apart from distinctness, TRIPS merely requires that the variety is sufficiently identifiable to allow for registration and protection, so there is some scope for a re-interpretation of the uniformity and stability requirements or for the setting up of 'second registers' for traditional and landraces.[44] Third, the *sui generis* legislation may link the granting of rights to proof of prior informed consent by the providers of germplasm.[45] In 2003, such a disclosure requirement was proposed by a group of developing countries in the Council for TRIPS as an amendment of the TRIPS Agreement to

---

[41] For an excellent summary of the pros and cons of adopting the different options for *sui generis* protection, *see* INTERNATIONAL PLANT GENETIC RESOURCES INSTITUTE (IPGRI), KEY QUESTIONS FOR DECISION-MAKERS: PROTECTION OF PLANT VARIETIES UNDER THE WTO AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS (1999), *available at* http://www.bioversityinternational.org/fileadmin/bioversity/publications/pdfs/41_Key%20questions%20for%20decision-makers.pdf.

[42] Dan Leskien & Michael Flitner, *Intellectual Property Rights and Plant Genetic Resources: Options for a Sui Generic System* (IPGRI, Issues in Genetic Resources No. 6, 1997), *available at* http://www.bioversityinternational.org/fileadmin/bioversity/publications/pdfs/497.pdf.

[43] *Id.* at 48-49.

[44] *Supra* note 42, at 53-54.

[45] *Supra* note 42, at 56.

harmonise the requirements under TRIPS with those under the CBD.[46] The proposal is since strongly debated in the various forums concerned with traditional knowledge. Industrialised countries have either opposed the proposal or adopted disclosure requirements that leave the remedies for failure to comply outside of the patent system and do not lead to revocation of patents.[47] Fourth, the scope of *sui generis* protection may range from rights via the 1991 and 1978 UPOV models to the use of PVP seals, depending on the needs and prospects for commercial plant breeding in a particular country.[48] Fifth, any *sui generis* legislation may be further supported by measures such as the establishment of community gene funds, registers and databases for forms of traditional knowledge and the creation of an office of public defender to mediate and intervene in conflicts between communities and national governments or between states and multinational corporations.[49] With a view to some of these options outside of UPOV, analysts have critically noted, however, that they will have to be assessed against the TRIPS requirement of Article 27.3(b) that an 'effective' *sui generis* system must be provided.[50]

VI

OTHER SUPPLEMENTARY MECHANISMS FOR THE PROTECTION OF TRADITIONAL KNOWLEDGE

There are other supplementary mechanisms to protect forms of traditional knowledge related to plant varieties and biodiversity that cannot be discussed in detail within the limited scope of this article. Some of these will be referred to again in the context of the case studies from Asia below. For example, geographical indications may be employed to bring about protection of traditional knowledge via symbols akin to trade marks, where other more direct measures of traditional

---

[46] *Supra* note 5, at 398. For a more detailed discussion, *see* DISCLOSURE REQUIREMENTS: ENSURING MUTUAL SUPPORTIVENESS BETWEEN THE WTO TRIPS AGREEMENT AND THE CBD (Martha Chouchena-Rojas et al. eds., 2005). For a view opposing such disclosure requirements, *see* Jon P. Santamauro, *Reducing the Rhetoric: Reconsidering the Relationship of the TRIPS Agreement, CBD and Proposed New Patent Disclosure Requirements Relating to Genetic Resources and Traditional Knowledge*, 29 EUR. INTELL. PROP. REV. 91 (2007).

[47] Brendan Tobin, *The Role of Customary Law and Practice in the Protection of Traditional Knowledge Related to Biological Diversity*, *in* TRADITIONAL KNOWLEDGE, TRADITIONAL CULTURAL EXPRESSIONS AND INTELLECTUAL PROPERTY LAW IN THE ASIA-PACIFIC REGION 127, 140 (Christoph Antons ed., 2009).

[48] *Supra* note 42, at 58-62.

[49] *Supra* note 42, at 64-65.

[50] *Supra* note 10, at 435; *see also supra* note 4, at 308 (Llewelyn nevertheless sees "scope for both imaginative interpretation and application."); *see also* Prabash Ranjan, *Recent Developments in India's Plant Variety Protection, Seed Regulation and Linkages with UPOV's Proposed Membership*, 12 J. WORLD INTELL. PROP. 219, 222-223 (2009) (suggesting that what is 'effective' should not be judged exclusively from the perspective of plant breeders, but also from the perspective of farmers).

knowledge protection fail.[51] Furthermore, there is the discussion, already mentioned above, about disclosure requirements for intellectual property rights applications that make use of forms of traditional knowledge.[52] Finally, there is an emerging debate about the importance of forms of customary law in the context of sustainable development in general[53] and in the context of traditional knowledge protection in particular.[54] It has been argued, among other things, that customary law could provide avenues to overcome the 'tragedy of the commons' theory that open access by self-interested individuals necessarily leads to over-exploitation of resources. Rather than moving to the opposite extreme of privatising resources, proponents of the role of customary law in sustainable development argue that many customary law systems operate with forms of limited common property,[55] where access to the resources is restricted, for example, to certain seasons or certain groups at certain times, thus avoiding overexploitation. The discussion about these issues in the context of traditional knowledge and intellectual property has only just begun and some reference to the use of customary law will be made in the case studies following. It is important to note, however, that customary law also faces many obstacles, such as limited recognition within the state systems of developing nations, the difficulties of creating representative bodies of customary law communities within the wider national and international setting, the concerns of human rights lawyers about some customary practices, the question of membership of local societies in an age of globalisation and extensive migration, and the general difficulties of adapting indigenous worldviews to the developmental agenda of an industrialising state.[56] Critics have pointed out that, at first, colonial policies and subsequently internal migration in post-colonial nation states mean that boundaries of customary communities are now difficult to draw and customary law would have to be resurrected from a long period of decline.[57] We will return to some of these issues in the context of the following case studies and in the conclusion to this article.

---

[51] *See* David R. Downes, *How Intellectual Property Could Be a Tool to Protect Traditional Knowledge*, *in* THE EARTHSCAN READER ON INTERNATIONAL AND SUSTAINABLE DEVELOPMENT (Kevin P. Gallagher & Jacob Werksman eds., 2002); Dwijen Rangnekar, *The Socio-Economics of Geographical Indications: A Review of Empirical Evidence from Europe* (UNCTAD-ICTSD, Project on IPRs and Sustainable Development Series – Issue Paper No. 8, 2004), *available at* http://ictsd.org/downloads/2008/07/a.pdf.

[52] *See supra* note 47.

[53] PETER OREBECH ET AL., THE ROLE OF CUSTOMARY LAW IN SUSTAINABLE DEVELOPMENT (2005).

[54] *See* WIPO, *Customary Law & the Intellectual Property System in the Protection of Traditional Cultural Expressions and Knowledge* (WIPO, Issues Paper, 2006), *available at*
http://www.wipo.int/tk/en/consultations/customary_law/issues.pdf

[55] For a detailed discussion, *see supra* note 53, at 12.

[56] For a discussion in relation to some of these problems, *see supra* note 53, at 338.

[57] Martin Chanock, *Branding Identity and Copyrighting Culture: Orientation Towards the Customary in Traditional Knowledge Discourse*, *in* TRADITIONAL KNOWLEDGE, TRADITIONAL CULTURAL EXPRESSIONS AND INTELLECTUAL PROPERTY LAW IN THE ASIA-PACIFIC REGION 177 (Christoph Antons ed., 2009). For different assessments of such problems based on

VII

EXAMPLES FROM ASIA

The following case studies from the Philippines and India represent two examples of the different approaches to traditional knowledge protection currently used in Asia. They range from traditional knowledge protection as part of a comprehensive protection of indigenous cultural rights, as in the Philippines, to the protection of specialised segments of traditional knowledge in the national interest, the approach adopted by the national government in India.

A. THE PHILIPPINES

1. The Intellectual Property Code and the Plant Variety Protection Act

Intellectual property legislation in the Philippines provides only limited recognition for forms of traditional knowledge. Section 22.4 of the Intellectual Property Code of the Philippines declares as non-patentable, plant varieties or animal breeds or essentially biological processes for the production of plants or animals other than micro-organisms and non-biological and microbiological processes. However, the provision explicitly leaves room for the enactment of *sui generis* protection for plant varieties and for a system of community intellectual rights protection. The *sui generis* option has meanwhile been exercised with the enactment of the Philippine Plant Variety Protection Act of 2002.[58] The Act follows the 1991 UPOV model. In section 43 (d), it protects the traditional right of small farmers to save, use, exchange, share or sell their farm produce of a protected variety, except when a sale is for the purpose of reproduction under a commercial marketing agreement. The availability of this exception is to be determined by the National Plant Protection Board. The provision further allows exchange and sale of seeds among small farmers for reproduction and replanting on their own land. Farming Communities and *bona fide* farmers' organisations are further encouraged to build inventories of locally bred varieties to safeguard them against misappropriation and monopolisation. NGOs have assisted local farming communities to establish and upgrade such community registers of their local and traditional varieties.[59]

---

fieldwork in Indonesia, *see also* TANIA MURRAY LI, THE WILL TO IMPROVE: GOVERNMENTALITY, DEVELOPMENT AND THE PRACTICE OF POLITICS (2007); Franz von Benda-Beckmann & Keebet von Benda-Beckmann, *Between Global Forces and Local Politics: Reorganisation of Village Government in Indonesia*, *in* GLOBALISATION AND RESISTANCE: LAW REFORM IN ASIA SINCE THE CRISIS (Christoph Antons & Volkmar Gessner eds., 2007).

[58] An Act to Provide Protection to New Plant Varieties, Establishing a National Plant Protection Board and for Other Purposes, Rep. Act 9168 (2002) (Phil.).

[59] ALYWIN D. M. ARNEJO, THE COMMUNITY REGISTRY AS AN EXPRESSION OF FARMERS' RIGHTS: EXPERIENCES IN COLLECTIVE ACTION AGAINST THE PLANT VARIETY PROTECTION ACT OF THE PHILIPPINES, *available at*

2. Bioprospecting under Executive Order No. 247

The Philippines has seen a new emphasis on the environment and on biological resources since the early post-Marcos years. Following the People Power Revolution of 1986, new President Corazon Aquino restructured and reformed the former Natural Resources Ministry, transforming it into the Department of Environment and Natural Resources.[60] Following the Earth Summit in Rio de Janeiro in 1992, Aquino's successor, Fidel Ramos, initiated the Philippine Commission on Sustainable Development (PCSD), which in turn translated the Earth Summit's Agenda 21 into the local Philippine version.[61] Also in 1992, Ramos established via RA No. 7586 the National Integrated Protected Areas System (NIPAS), which designated ecologically sensitive areas such as sanctuaries, reserves and natural parks.

This was followed by Executive Order No. 247 "Prescribing a Regulatory Framework for the Prospecting of Biological and Genetic Resources, their By-Products and Derivatives, for Scientific and Commercial Purposes, and for Other Purposes" of May 1995 (EO 247) and by the DENR implementing regulations for this order DAO 96-20. EO 247 was deliberately drafted in the form of Executive Order rather than as a legislative bill to take advantage of the supportive climate for such legislation under the Ramos administration.[62] EO 247 covered all types of biodiversity collection, except for traditional use, and it created the Inter-Agency Committee on Biological and Genetic Resources (IACBGR). Parties interested in bio prospecting in the Philippines had to enter into a research agreement with a relevant government department on recommendation of the IACBGR. EO 247 distinguished between commercial research agreements and academic research agreements. It foresaw certain minimum requirements for commercial research agreements, including provision for royalty payments, provision of information about discoveries with a commercial value, involvement of Philippine researchers in research conducted by foreigners and termination of the agreement after a maximum of three years. Only duly recognised Philippine universities, academic institutions, domestic and intergovernmental entities were allowed to apply for a renewable academic research agreement with a maximal duration of five years. Prior informed

---

http://www.capri.cgiar.org/pdf/GRarnejo.pdf (paper presented at the CAPRi-IPGRI International Workshop on Property Rights, Collective Action and Local Conservation of Genetic Resources, Rome (2003)).

[60] WALDEN BELLO ET AL., THE ANTI-DEVELOPMENT STATE: THE POLITICAL ECONOMY OF PERMANENT CRISIS IN THE PHILIPPINES 218 (2004). For a discussion on the policy shifts within DENR under the various administrations, *see* Marites Danguilan-Vitug, *Forest Policy and National Politics*, *in* FOREST POLICY AND POLITICS IN THE PHILIPPINES: THE DYNAMICS OF PARTICIPATORY CONSERVATION 11-39 (Peter Utting ed., 2000).

[61] BELLO, *id.* at 219; *see also* DEVELOPING THE NATIONAL BIOSAFETY FRAMEWORK FOR THE PHILIPPINES 48 (S. Halos et al. eds., 2004).

[62] KRYSTYNA SWIDERSKA ET AL., DEVELOPING THE PHILIPPINES EXECUTIVE ORDER NO. 247 ON ACCESS TO GENETIC RESOURCES 15 (2001), *available at* http://www.cbd.int/doc/case-studies/abs/cs-abs-order-ph-en.pdf.

consent of indigenous cultural communities in accordance with customary law was required. While monitoring on the ground was the responsibility of the Protected Areas and Wildlife Bureau (PAWB) of DENR, the IACBGR recommended the approval of applications to the relevant Department Secretaries, decided on the amount of material to be taken and monitored observance of the conditions of the agreements, especially compliance with conditions imposed for the protection of indigenous and local communities. The Inter-Agency Committee consisted primarily of staff drawn from the Departments of Environment and Natural Resources, Science and Technology, Agriculture, Health and Foreign Affairs, joined by two scientists and representatives of the National Museum, as well as representatives from an NGO and from a People's Organization (PO) representing indigenous cultural communities.

3. The Indigenous Peoples' Rights Act

One initial criticism of EO 247 and its implementing regulations was the rather paternalistic manner of obtaining the prior informed consent of affected communities.[63] In this regard, section 7 of the implementing rules and regulations in DAO 96-20 merely foresaw public notification and consultation with relevant officials and government agencies. More detailed provisions regarding the prior informed consent of indigenous people in particular followed from specialised legislation, enacted in 1997 and covering the rights of indigenous people. In the context of Asian governments' policies regarding indigenous people and local minorities, the Philippines is a rather exceptional case. The concept of indigenous people has a long history in this country and is constitutionally recognised.[64] The distinction between Christianised Filipinos or *Indios*, Muslim Filipinos or *Moros* and the indigenous non-Christian tribes or *infieles* goes back to the Spanish colonial period.[65] Rule by the United States after 1898 further strengthened the separate administration of the so-called 'uncivilized tribes' of the archipelago, for which President McKinley prescribed "the same course followed by Congress in permitting the tribes of our North American Indians to maintain their tribal organization and government."[66] From 1903, Bureau of Non-

[63] Oscar B. Zamora, *The Philippines: A Bridle on Bioprospecting?*, SEEDLING, June 1997, *available at* http://www.grain.org/seedling/index.cfm?id=13.

[64] On the historical backgound, *see* Gerard A. Persoon, *Being Indigenous in Indonesia and the Philippines*, *in* TRADITIONAL KNOWLEDGE, TRADITIONAL CULTURAL EXPRESSIONS AND INTELLECTUAL PROPERTY LAW IN THE ASIA-PACIFIC REGION 195, 207-209 (Christoph Antons ed., 2009).

[65] A discussion of the historical development of these classifications can be found in *Isagani Cruz & Anr. v. Sec'y of Env't & Natural Res. & Ors.*, G.R. No. 135385, (S.C. December 6, 2000) (Phil.) (separate opinion of Puno, J., *available at* http://sc.judiciary.gov.ph/jurisprudence/2000/dec2000/135385_puno.htm); *see also* R. J. May, *Ethnicity and Public Policy in the Philippines*, *in* GOVERNMENT POLICIES AND ETHNIC RELATIONS IN ASIA AND THE PACIFIC 321, 324 (Michael Brown & Sumit Ganguly eds., 1997).

[66] *Id.*

Christian tribes became responsible for their administration. Interestingly, the responsibility of this agency extended not only to animist indigenous people, but also to the *Moros* of the Mindanao and Sulu islands in the South of the Philippines.[67] After independence, attempts at assimilation and integration were made and the 'cultural communities' were constitutionally recognised in the Constitutions of 1973 and 1987. Today, the National Commission on Indigenous Peoples (NCIP) identifies 95 distinct tribes in 14 regions of the country with an estimated population of 12-15 million people.[68] A World Bank study of 2007 pointed, however, to difficulties in establishing such figures and to discrepancies between lists of indigenous peoples drafted by various institutions, for example, because of different use of ethnic names or labels.[69]

Against this background, it is perhaps less surprising that the Philippines is the only country in Asia that has made serious attempts to implement protection for a holistic notion of 'community intellectual rights' and 'cultural and intellectual rights' with elements of both traditional resource rights and folklore. The vehicle for this protection is currently the Indigenous Peoples Rights Act of 1997 (IPRA). At the time of its enactment, the IPRA was hailed as landmark legislation in this area of law in Asia. It provided broad recognition for the rights of Indigenous Cultural Communities/ Indigenous Peoples (ICC/IPs) to their ancestral domains and to the development of their cultures, traditions and institutions. To facilitate the exercise of these rights, the recognition of native title in Ancestral Domains and the granting of Certificates of Ancestral Domain Title (section 11, IPRA) were required.

Section 5 of the Act explains that the indigenous concept of ownership holds that ancestral domains are the ICCs/IPs' private but community property, which belongs to all generations and cannot be sold, disposed or destroyed.[70] This concept also covers traditional resource rights. Traditional resource rights are further defined in section 3 (o) as the "rights of ICCs/IPs to sustainably use, manage, protect and conserve (a) land, air, water, and minerals; (b) plants, animals

---

[67] James Eder & Thomas McKenna, *Minorities in the Philippines: Ancestral Lands in Theory and Practice*, *in* CIVILIZING THE MARGINS: SOUTHEAST ASIAN GOVERNMENT POLICIES FOR THE DEVELOPMENT OF MINORITIES 56, 60-61 (Christopher R. Duncan ed., 2004); May, *supra* note 65, at 331.

[68] Jose Mencio Molintas, *The Philippine Indigenous Peoples' Struggle for Land and Life: Challenging Legal Texts*, 21 ARIZ. J. INT'L & COMP. L. 269, 272 (2004).

[69] Josefo B. Tuyor et al., *The Indigenous Peoples Rights Act: Legal and Institutional Frameworks, Implementation and Challenges in the Philippines* 34-35 (Sustainable Dev. Dep't, E. Asia & Pac. Region, World Bank, Discussion Paper, 2007); Persoon, *supra* note 64, at 206 (quotes estimates from the International Working Group for Indigenous Affairs of 8-10 million indigenous people in the Philippines).

[70] *See also* § 3, Rule III (Part I), NCIP – Administrative Order No. 1/1998 (Phil.).

and other organisms; (c) collecting, fishing and hunting grounds; (d) sacred sites; and (e) other areas of economic, ceremonial and aesthetic value in accordance with their indigenous knowledge, beliefs, systems and practices."[71] The rights to ancestral domains include, according to section 7 (a), the right to claim ownership over lands, bodies of water traditionally and actually occupied by ICCs/IPs, sacred places, and traditional hunting and fishing grounds. The right to develop lands and natural resources in section 7 (b) includes the following:

- the right to develop, control and use lands and territories traditionally occupied, owned or used;
- the right to manage and conserve natural resources within the territories and uphold the responsibilities for future generations;
- the right to benefit and share the profits from allocation and utilization of the natural resources found within the territory;
- the right to negotiate the terms and conditions for the exploration of natural resources in the areas for the purpose of ensuring ecological, environmental protection and the conservation measures in accordance with national and customary laws;
- the right to an informed and intelligent participation in project formulation and implementation and to receive just and fair compensation for any damages;
- the right to effective government measures to prevent any interference with, alienation and encroachment upon these rights.

A further and more detailed definition of these rights can be found in Rule III, Part II, Section 2 of NCIP Administrative Order No. 1 of 1998. According to section 2 (a) of this Order, at least 30 per cent of funds received will be allocated to the ICC/IP community for development projects or provision of social services or infrastructure in accordance with their Ancestral Domain Sustainable Development and Protection Plan (ADSDPP).

In cases of conflict, section 7 (h) gives priority to customary law as a means for conflict solving with amicable settlement and judicial procedures in the courts of justice as default mechanisms. This is further specified in Rule III, Part II, Section 8 of NCIP Administrative Order No. 1 of 1998, according to which conflicts unresolved under customary law are submitted to the NCIP and may be appealed to the Court of Appeals. Rule IV, Part I, Section 4 indicates that the traditional justice

[71] *See also* § 2, Rule III (Part II), NCIP - Administrative Order No. 1/1998 (Phil.) (refers to the Ancestral Domain Sustainable Development and Protection Plan (ADSDPP)).

systems are recognised as long as they are compatible with national laws and accepted international human rights.

The most important rights relating to intellectual property and biological resources are to be found in Chapter VI of the Act under the heading 'Cultural Integrity.' Section 29 states generally that the State shall respect, recognise and protect the rights of ICCs/IPs to preserve and protect their culture. Section 32 guarantees 'Community Intellectual Rights' including those of various manifestations of culture and the right to restitution of cultural, intellectual, religious and spiritual property taken in an unauthorised manner and without prior informed consent.

Section 34 of Chapter VI further provides that ICCs/IPs are:

> entitled to the recognition of full ownership and control and protection of their cultural and intellectual rights. They shall have the right to special measures to control, develop and protect their sciences, technologies and cultural manifestations, including human and other genetic resources, seeds, including derivatives of these resources, traditional medicines and health practices, vital medicinal plants, animals and minerals, indigenous knowledge systems and practices, knowledge of the properties of fauna and flora, oral traditions, literature, designs, and visual and performing arts.

A similar, but more extended definition of 'community intellectual rights' is given in Rule II, Section 1 (j) of the NCIP implementing Administrative Order No. 1 of 1998. Accordingly, community intellectual rights include:

> rights of ICCs/IPs to own, control, develop and protect: (a) the past, present and future manifestations of their cultures, such as but not limited to, archaeological and historical sites, artefacts, designs, ceremonies, technologies, visual and performing arts and literature as well as religious and spiritual properties; (b) science and technology, including but not limited to, human and other genetic resources, seeds, medicine, health practices, vital medicinal plants, animals and minerals, indigenous knowledge systems and practices, resource management systems, agricultural technologies, knowledge of the properties of fauna and flora, oral traditions, designs, scientific discoveries; and (c) language, script, histories, oral traditions and teaching and learning systems.

Indigenous knowledge systems and practices are in turn defined in Rule II, Section 1 (p) of Administrative Order No. 1 of 1998 as:

> systems, institutions, mechanisms and technologies comprising a unique body of knowledge evolved through time that embody patterns of relationships between

> and among peoples and between peoples, their lands and resource environment, including such spheres of relationships which may include social, political, cultural, economic, religious spheres, and which are the direct outcome of the indigenous peoples' responses to certain needs consisting of adaptive mechanisms which have allowed indigenous peoples to survive and thrive within their given socio-cultural and biophysical conditions."

The same definitions return once again in Rule VI of Administrative Order No. 1 of 1998. This time 'community intellectual property rights' as well as the 'right to protection of indigenous knowledge systems and practices' are listed among the right to cultural integrity (Rule VI, Section 3). The definitions used in Rule IV, Sections 10 and 14 are largely identical to those elsewhere in the order except that section 10 (c) adds 'music, dances, conflict resolution mechanisms, peace building processes' and 'life, philosophy and perspectives' to the term 'community intellectual property.' The rights are to be established in accordance with the Convention on Biodiversity, the Universal Declaration of Indigenous Peoples' Rights and the Universal Declaration of Human Rights. Administrative Order No. 1 foresees different procedures for research permits (Rule IV, Section 15) and for joint undertakings with commercial ventures (Section 17). Violations of the free and prior informed consent regulations will be subject to penalties under customary law and fines under both the Indigenous Peoples' Rights Act and Administrative Order No. 1 of 1998. However, if customary law is applied, cruel, degrading or inhuman penalties, the death penalty and excessive fines are prohibited (Rule XI, Part III, Section 1 of Administrative Order No. 1 of 1998 and section 72 of the Indigenous Peoples Rights Act).

Section 35 requires the free and prior informed consent of the communities in accordance with customary laws for access to biological and genetic resources, and section 36 encourages the recognition and promotion of sustainable agro-technological development among ICCs/IPs. The manner of obtaining free and prior informed consent is regulated in detail in Rule IV, Part III of the NCIP Administrative Order No. 1 of 1998. Section 7 of this part mentions examples where these procedures have to be followed, including the "exploration, development, exploitation and utilization of natural resources within ancestral domains/lands" and "research in indigenous knowledge, systems and practices related to agriculture, forestry, watershed and resource management systems and technologies, medical and scientific concerns, bio-diversity, bio-prospecting and gathering of genetic resources." Furthermore, section 8 foresees a Memorandum of Agreement between proponent, the host ICC/IP community and the NCIP covering benefits, measures to protect community rights, responsibilities of all parties, conditions in case of change

of proponent where appropriate, and penalties for non-compliance and violations of the terms and conditions.

The Act further created a National Commission on Indigenous Peoples with legislative and executive powers as the main representative body for indigenous interests. According to section 44 of the Act, the powers of the NCIP include the granting of certificates of ancestral domain title; the entering into contracts and agreements to achieve the objectives of the Act; the granting of permits to dispose, utilise, manage and appropriate parts of the ancestral domain with the approval of the ICCs/IPs; the decision about appeals regarding its own decisions and acts and the promulgation of implementing rules and regulations. The main set of implementing regulations followed in 1998 via Administrative Order No. 1 of the NCIP.

While Administrative Order No. 1 of the NCIP regulated the implementation of the IPRA in general, Administrative Order No. 3 brought specific guidelines for free and prior informed consent. In 2002, the NCIP issued a revised Administrative Order No. 3 concerning revised guidelines for the issuance of certification precondition and the free and prior informed consent.[72] This order was again repealed by NCIP Administrative Order No. 1 of 2006. This latest implementing regulation distinguished between certification precondition issued by the NCIP for projects that have met all requirements of free and prior informed consent and certificates of non-overlap for projects that do not affect indigenous peoples or that fall outside of ancestral domains.[73]

4. The Traditional and Alternative Medicine Act

Further legislation introduced in 1997: Republic Act No. 8423 of 1997 covers aspects of traditional knowledge and created the Philippine Institute of Traditional and Alternative Health Care (PITAHC) to accelerate the development of traditional and alternative health care in the Philippines. It provides for a Traditional and Alternative Health Care Development Fund for these and other purposes.[74] However, much of this legislation is in fact concerned with the integration of traditional and alternative health care into the national health care system and with safety standards, coordination and guidelines for such medicines. The inclusion of a definition of

[72] *See* NCIP Administrative Order No. 3/2002 (Phil.).

[73] Tuyor et al., *supra* note 69, at 13.

[74] An Act Creating the Phillipine Institute of Traditional and Alternative Health Care (PITAHC) to Accelerate the Development of Traditional and Alternative Health Care in the Philippines, Providing for a Traditional and Alternative Health Care Development Fund and for Other Purposes, Rep. Act 8423 (1997) (Phil.).

'alternative health care modalities' specifically acknowledges that the Act is not confined to indigenous knowledge and not even necessarily to knowledge having a long tradition in the Philippines. In spite of occasional references to indigenous societies and the requirement in section 2 to acknowledge their contributions and to pay royalties to them, the Act does not establish any specific mechanisms for this purpose. The Act defines 'traditional healers' as 'the relatively old, highly respected people with a profound knowledge of traditional remedies.' While traditional healers and environmental sector organisations are represented on the Board of the Philippine Institute of Traditional and Alternative Health Care, there is no specific representation of indigenous communities.

5. New bioprospecting guidelines under Administrative Order No. 1 of 2005

On paper, the Philippines had a sophisticated bio prospecting and traditional knowledge system by the late 1990s. In practice, however, implementation of the legislation was disappointing and slow. Swiderska, Dano and Dubois report only two approvals for research agreements under EO 247 between 1995 and 2001, one of a commercial and one of an academic nature.[75] Developments under the IPRA were not much better. In fact, the IPRA faced a constitutional challenge shortly after its enactment. The petition failed after an evenly divided Supreme Court upheld the legislation in 2000.[76] Land claims remained suspended during this period, however, so that the implementation of the IPRA was delayed considerably.[77] According to a World Bank study of 2007, the NCIP issued 29 certificates of ancestral domain titles from 2002 to 2004. Among the reasons for the relatively slow progress in issuing these certificates, the study cited lack of technical expertise in boundary delineation, lack of financial and logistical resources and disputes about ancestral domains between indigenous and non-indigenous communities as well as among different groups of indigenous peoples.[78]

From 2001 onwards, the new Arroyo administration issued various pieces of legislation that attempted to harmonise and centralise the dispersed legislation on access to biological resources. Republic Act No. 9147 "providing for the conservation and protection of wildlife resources and their habitats, appropriating funds therefore and for other purposes" distinguished again between

---

[75] SWIDERSKA ET AL., *supra* note 62, at 28; *see also* Cecile Dumol, New Bioprospecting Guidelines in the Philippines (June 28, 2005), http://www.pchrd.dost.gov.ph/index.php/news-archive/70 (last visited July 9, 2010).

[76] *See* Isagani Cruz & Anr. v. Sec'y of Env't & Natural Res. & Ors., G.R. No. 135385, (S.C. December 6, 2000) (Phil.), *available at* http://sc.judiciary.gov.ph/jurisprudence/2000/dec2000/135385.htm.

[77] Eder & McKenna, *supra* note 67, at 67.

[78] Tuyor et al., *supra* note 69, at 48.

bio prospecting for commercial and for scientific purposes. Since this Act concerned collection activities within all areas of the country, including areas under the National Integrated Protected Areas System, these areas potentially overlapped with the ancestral domains and lands under the IPRA, a problem that had already been recognised in the original NIPAS legislation.[79] DENR and NCIP now jointly issued a memorandum for the harmonisation of the implementation of IPRA and Environmental and Natural Resources Laws and Policies.[80]

Administrative Order No. 1 of 2005, a further joint initiative of the DENR, the Department of Agriculture (DA), the Palawan Council for Sustainable Development (PCSD) and the NCIP, brought a new set of guidelines for bio prospecting in the Philippines. They apply to all bio prospecting activities in the Philippines and to *in situ* as well as to *ex situ* collections. The guidelines also clarify that they apply to all areas, including ancestral domains and lands that are subject to the IPRA. Prior informed consent is to be obtained either from ICCs/IPs or, in the case of non-indigenous local communities, from a *Barangay* Assembly.[81]

Under the new guidelines, each bio prospector has to conclude a Bio prospecting Undertaking (BU) with the DENR and/or the DA, represented by its respective Departmental Secretary. There is a special regulation for activities in the Province of Palawan, where the BU must be co-signed by the Chairperson of the PCSD. The implementation is largely in the hands of the various departmental agencies. As for indigenous ancestral domains and lands, the NCIP shall assist with obtaining the prior informed consent of indigenous people and in the negotiation of benefit sharing agreements. The rules and regulations of the IPRA are to be followed for the securing of prior informed consent. As for benefit sharing agreements, a minimum bio prospecting fee, which may be higher if traditional knowledge is concerned, will go to the national government. Royalties are to be shared between the national government and local governments, if that are foreseen by local government regulation. Representatives of the various resource providing communities negotiate the benefit sharing agreements and these communities also receive any up-front payments. The bio prospecting fee will be used for a Wildlife Management or Protected Area

---

[79] *See* An Act Providing for the Establishment and Management of National Integrated Protected Areas System, Defining its Scope and Coverage, and for Other Purposes, Rep. Act 7586, § 13 (1992) (Phil.).

[80] *See* Joint DENR-NCIP Memorandum Circular No. 2003-1 on Harmonization of the Implementation of the Indigenous Peoples Rights Act (IPRA) and Environment and Natural Resources (ENR) Laws and Policies (Oct. 31, 2003), *available at* http://www.mgb.gov.ph/Files/Policies/DENR-NCIP%20MC%202003-1.doc.

[81] The Barangay Assembly represents a 'barangay', a traditional Philippine administrative unit, usually consisting of between 100 to 500 families, *see* JURGEN RULAND, POLITIK UND VERWALTUNG IN METRO MANILA – ASPEKTE DER HERRSCHAFTSSTABILISIER UNG IN EINEM AUTORITAREN POLITISCHEN SYSTEM 120 (1982).

Fund. However, if the fee is collected for activities in areas under the IPRA, the IPRA also regulates the manner in which the funds will be used. DENR Administrative Order 96-20 is repealed, as is Executive Order No. 247 in so far as it is inconsistent with the Wildlife Act. The Inter-Agency Committee on Biological and Genetic Resources is dissolved and its functions are now exercised by the Secretary of the DENR or DA. Apart from royalties and fees, there is also provision for a rehabilitation/performance bond amounting to 25 per cent of the project cost as reflected in the research budget. This is to be posted before the bio prospecting activities begin.

The new guidelines foresee a compliance monitoring system via annual progress reports and various certifications for prior informed consent, benefit sharing and collection quotas. Forms for these purposes are to be found in Annexes to the Administrative Order. Monitoring overseas is to be undertaken by DFA and DOST. NGOs and POs are equally encouraged to participate in the monitoring process. Non-compliance with the BU will lead to cancellation/revocation of the agreement, confiscation of the material, forfeiture of the rehabilitation and performance bond, imposition of a perpetual ban on access to biological resources in the Philippines and imposition of administrative and criminal sanctions under the Wildlife Act. There is a further provision allowing for the 'shaming' of the violator in national and international media and the reporting of the violations to international and regional monitoring bodies. There is nothing, however, in either the Intellectual Property Code of the Philippines or in Administrative Order No. 1 of 2005 providing for the revocation of a patent that has made use of knowledge and of material obtained under circumstances that violated one or more of the prior informed consent, benefit sharing and collection quota requirements.

The guidelines exempt scientific research on agro-biodiversity and scientific research on wildlife under section 15 of the Wildlife Resources and Conservation Protection Act from the application of the guidelines, but in the latter case they subject any further transfer of material for commercial purposes to the guidelines. Also exempted is traditional use and subsistence consumption as well as use of *ex situ* collections, which are covered by international agreements. Finally, the development of medicinal plants for traditional and alternative medicine is primarily governed by the Traditional and Alternative Medicine Act.

For all other bio prospecting purposes, which are defined as "research, collection and utilization of biological and genetic resources for purposes of applying the knowledge derived there from solely for commercial purposes", the bio prospecting guidelines apply and the BU has to make reference

to certain standard terms and conditions contained in Annex I to the Guidelines. These conditions are very similar to those requested previously under EO 247. Thus, specimens are to be deposited with various agencies in the Philippines, research is to be in collaboration with Philippine agencies, ownership is to be retained by the Philippines of all material, and if there are third party recipients, a material transfer agreement with specified content is to be reached. While many of these conditions are compulsory,[82] some give preference to the BU or the benefit sharing agreement. Section 9 of the Standard Terms and Conditions requires that "all discoveries and commercial products made or derived from Philippine biological resources shall be made available to the Philippine government and resource provider", but only "as may be agreed upon in the BU." Equally, section 11 requires the royalty-free licensing of technology derived from Philippine endemic species to the Philippine government through a designated Philippine institution but provides further that "where appropriate and applicable, other terms may be negotiated by the parties." In the case of germplasm exchange, the technology shall be shared with the collaborating National Agricultural Research systems in line with mission statements of such centres and in accordance with protocols under international law.

According to the Philippines' 4th National Report to the Convention on Biological Diversity of 2009, NCIP records show that indigenous communities had benefitted by 2007 from 199 projects in various areas. However, until 2009 no access application had been processed under the 2005 bio prospecting guidelines of Joint Administrative Order No. 1. The report identified as the reason for the lack of applications, the perception that the regulation was restricting research and the royalty provisions were a disincentive to research. Consequently, the report identified "an urgent need to review provisions in the regulation in order to address the concerns of both researchers and regulators."[83] According to the same report, progress has been made, however, with regards to the nationwide documentation of indigenous knowledge systems and practices.[84] Administrative Guidelines to regulate such activities for sustainable traditional and indigenous forest resources management systems and practices have meanwhile been issued in DENR-NCIP Joint Administrative Order No. 1 of 2008.

---

[82] *See* § 9.1, Joint DENR-DA-PCSD-NCIP Administrative Order No. 1/2005 (Phil.) ("The BU shall contain, in addition to the negotiated terms of benefit-sharing, standard terms and conditions relating to compliance with complementary regulations and other basic contractual terms. These terms and conditions are listed in Annex I.").

[83] REPUBLIC OF THE PHILIPPINES, ASSESSING PROGRESS TOWARDS THE 2010 BIODIVERSITY TARGET: THE 4TH NATIONAL REPORT TO THE CONVENTION ON BIOLOGICAL DIVERSITY 65 (2009), *available at* http://www.cbd.int/doc/world/ph/ph-nr-04-en.pdf.

[84] *Id.* at 66.

6. The Draft Bill for Community Intellectual Rights Protection

Finally, a far-reaching Draft Bill for Community Intellectual Rights Protection was introduced in 2001. Protection extends to parent strains and genetic material discovered or selected and conserved by local communities; seeds and reproductive material, agricultural practices and devices, medicinal products and processes, cultural products from local communities and all other products or processes discovered through a community process. While the draft on the one hand recognises indefinite rights to the material, royalties for registered forms of traditional knowledge may only be collected for ten years. Among the beneficiaries of the draft legislation are 'farmer-innovators', defined as:

> i. an individual who has provided or was the source of parent strains used in the development of a new variety; ii. the local community, which has helped to conserve and develop the genetic stocks which have gone into the pedigree of a new variety; iii. the residents of an area rich in plant genetic resources from where breeders or breeding institutions responsible for the new variety have obtained donors of genes for resistance/tolerance/avoidance to biotic and/or abiotic stress or other valuable character.

This draft is based on model legislation developed by the Third World Network and is apparently still under consideration in the Philippine Senate, where it has been pending for some years.[85]

B. INDIA

Indian policy makers seem torn between high technology ambitions in areas such as biotechnology and the need to account for a large rural sector.[86] The move from traditional to commercial farming is still a matter of hefty debate in India. Many Indian farmers have become heavily indebted. Press reports indicate that 95 per cent of cotton farmers are struggling with heavy debt and that an unusual large number have committed suicide over the past few years.[87] At the same time, commercial farming in India has been boosted by a number of new laws and amendments, which India had to enact as a result of the country's accession to the WTO-TRIPS Agreement. The Indian Government has also taken steps to accede to the UPOV Convention, but these accession

---

[85] Draft Bill – Community Intellectual Rights Protection Act (July 24, 2008), http://www.grain.org/brl/?docid=767&lawid=1469 (last visited July 9, 2010).

[86] Anand Giridharadas, *Growing in India: Food for the World*, N.Y. TIMES, May 26, 2006, *available at* http://www.nytimes.com/2006/05/26/business/worldbusiness/26iht-wbfood.1829800.html; K. S. Jayaraman, *India Biotech Boom*, 436 NATURE 480 (2005); K. P. Prabhakaran Nair, *Seeds Bill: A rich harvest for MNCs?*, HINDU BUS. LINE, Mar. 30, 2005, *available at* http://www.thehindubusinessline.com/2005/03/30/stories/2005033000240900.htm.

[87] Amelia Gentleman, *Despair takes toll on Indian farmers*, N.Y. TIMES, May 31, 2006, *available at* http://www.nytimes.com/2006/04/18/world/asia/18iht-farmers.1557902.html.

plans have remained controversial and their current status is unclear.[88] The following part of this article will discuss changes to laws as well as newer laws and draft laws related to plant varieties and to associated traditional knowledge. These include amendments to the Indian Patents Act, the Protection of Plant Varieties and Farmers' Rights Act, the Biological Diversity Act, the Seeds Bill introduced in 2004 and the most recent Protection, Conservation and Effective Management of Traditional Knowledge Relating to Biological Diversity Rules, 2009.

1. The Indian Patents Act

The Patents Act of 1970 originally excluded methods of agriculture or horticulture from patentability (section 3(h)). Equally excluded were "any processes for the medicinal, surgical, curative, prophylactic or other treatment of human beings or any process for a similar treatment of animals or plants to render them free of disease or to increase their economic value or that of their products" (section 3(i)). The Indian courts further interpreted the term "manner of manufacture" in a restrictive way as exclusively related to processes resulting in non-living tangible products. This approach was only overturned in 2002 in *Dimminaco AG v. Controller of Patents*.[89] For inventions related to substances intended for use or capable of being used as food or medicine or drug and to substances prepared or produced by chemical processes, only process patent protection was given; no product patent was available (section 5).[90]

With India's entry into the WTO, transitional measures such as mailbox applications and exclusive marketing rights were introduced at first via an ordinance and then via amendments to the Patents Act in 1999.[91] In 2002, the Indian Patents Act was substantially amended. Section 3(c) referring to discoveries of scientific theory was extended to the "discovery of any living thing or non-living substance occurring in nature." The phrase has been interpreted restrictively as not including the isolation and purification of living substances or non-living substances involving human intervention.[92] The reference to plants in section 3(i) was omitted, and a new exclusion clause 3(j) was added covering "plants and animals in whole or any part thereof other than micro-organisms but including seeds, varieties and species and essentially biological processes for

---

[88] Ranjan, *supra* note 50, at 230-234.

[89] Shanti Kumar et al., *India: Patent regime comes of age*, MANAGING INTELL. PROP., October 2006: Supplement – Asia-Pacific IP Focus 2006, *available at* http://www.managingip.com/Article.aspx?ArticleID=1321297.

[90] *See* Philippe Cullet, *Property Rights over Biological Resources: India's Proposed Legislative Framework*, 4 J. WORLD INTELL. PROP. 211 (2001).

[91] Shanti Kumar & Neeti Wilson, *Biotechnology in the limelight*, MANAGING INTELL. PROP., April 2006: Supplement – Life Sciences 2006, *available at* http://www.managingip.com/Article.aspx?ArticleID=1321387.

[92] *Supra* note 89.

production or propagation of plants and animals." Commentators have pointed out that the section, in spite of the negative terms in which it is couched, in fact would allow the patenting of not only micro-organisms, but also of biotechnological process inventions requiring substantial human intervention.[93] Importantly, section 3(p) added a further exemption from patentability for "an invention which, in effect, is traditional knowledge or which is an aggregate or duplication of known properties of traditionally known component or components." Section 25(j) provides ground for opposition and section 64(p) the new revocation ground "that the complete specification does not disclose or wrongly mentions the source or geographical origin of biological material used for the invention." Under sections 25(k) and 64 (q), the ground for opposition and revocation is "that the invention so far as claimed in any claim of the complete specification was anticipated having regard to the knowledge, oral or otherwise, available within any local or indigenous community in India or elsewhere."[94] Also newly worded is section 3(b), which henceforth holds non-patentable "an invention the primary or intended use or commercial exploitation of which would be contrary to public order or morality or which causes serious prejudice to human, animal or plant life or health or to the environment." The Indian Patent Office has interpreted this as including "method(s) of adulteration of food."[95]

Another amendment followed in 2005, which abolished with section 5 the restriction to process patents for substances and made product patents available.[96] Because of the looming deadline of 1 January, 2005 for TRIPS compliance, this latest amendment was initially introduced via an ordinance and then signed into law in March 2005.[97] Currently still controversial is in particular section 3(d) of the amended Patents Act declaring as not patentable "the mere discovery of a new form of a known substance which does not result in the enhancement of the known efficacy of that substance or the mere discovery of any new property or new use of a known substance or of

---

[93] *Supra* note 91; *see also* Vandana Shiva, The Indian Seed Act and Patent Act: Sowing the Seeds of Dictatorship (Feb. 14, 2005), http://www.grain.org/bio-ipr/?id=431 (last visited July 8, 2010); *see also* Swati Gola, IMC India –The Patent Bill 2005: Impact on Agriculture (Mar. 22, 2005), http://india.indymedia.org/en/2005/03/210277.shtml (last visited July 8, 2010).

[94] On the 2002 amendments, *see* S. K. Verma, *Plant Genetic Resources, Biological Inventions and Intellectual Property Rights: The Case of India*, *in* INTELLECTUAL PROPERTY AND BIOLOGICAL RESOURCES 128, 147-148 (Burton Ong ed., 2004).

[95] *See* Robyn Ott, *Patentability of Plants, Animals and Microorganisms in India*, 2 OKLA. J.L. & TECH. 17 (2004).

[96] *See* the Patents (Amendment) Act, 2005, No. 15 of 2005; *see also* Gola, *supra* note 93.

[97] Rajnish Kumar Rai, *Patentable Subject Matter Requirements: An Evaluation of Proposed Exclusions to India's Patent Law in Light of India's Obligations Under the TRIPS Agreement and Options for India*, 8 CHI.-KENT J. INTELL. PROP. 41, 42 (2008); Emma Barraclough, *India patent reform under attack*, MANAGING INTELL. PROP., February 2005; Donald G. McNeil, Jr., *India alters law on drug patents*, N.Y. TIMES, Mar. 24, 2005, *available at* http://www.nytimes.com/2005/03/24/international/asia/24aids.html.

the mere use of a known process, machine or apparatus unless such known process results in a new product or employs at least one new reactant." The subsequent debate about "second medical uses" led to a court challenge to the constitutionality and TRIPS compatibility of section 3(d) by Swiss pharmaceutical manufacturer Novartis, which was dismissed in 2007.[98] The remainder of the challenge regarding the rejection of the patent application was recently rejected by the Intellectual Property Appellate Board (IPAB), which hears appeals from decisions of the Registrar of Trademarks and Geographical Indications as well as from the Controller of Patents.[99] Controversially also mentioning the cost factor of the drug as being detrimental to patent protection,[100] the IPAB based its decision mainly on section 3(d) holding that the free form of the drug was known and that "enhanced efficacy" of the new drug over the know substance had not been demonstrated.[101]

The controversial section 3(d) was also one of the subjects of the report of the Mashelkar Committee, an expert committee appointed to examine whether it would be TRIPS compatible to: a) limit the grant of a patent for pharmaceutical substances to new chemical entities or to new entities involving one or more inventive steps; and b) to exclude micro-organisms from patenting. The Committee concluded in its report that such a limitation of the patent would exclude an entire class of incremental innovations from patenting and would not be TRIPS compliant. It would equally not be TRIPS compliant to exclude micro-organisms from patenting.[102]

2. The Protection of Plant Varieties and Farmers' Rights Act

India's reaction to the requirements of Article 27.3(b), TRIPS is the Protection of Plant Varieties and Farmers' Rights Act (PPVFRA) of 2001. The Act follows largely the 1978 UPOV model, but commentators have pointed out that it also includes elements of the 1991 UPOV version, such as

---

[98] Novartis refuses to back down in Indian patent dispute (Jan. 8, 2007), http://www.managingip.com/Article/1257402/Novartis-refuses-to-back-down-in-Indian-patent-dispute.html (last visited July 8, 2010); Amelia Gentleman, *Setback for Novartis in India Over Drug Patent*, N.Y. TIMES, Aug. 7, 2007, *available at* http://www.nytimes.com/2007/08/07/business/worldbusiness/07drug.html; Linda L. Lee, *Trials and TRIPS-ulations: Indian Patent Law and Novartis AG v. Union of India*, 23 BERKELEY TECH. L.J. 281, 299 (2008).

[99] Lee, *id.* at 287-288.

[100] Rahul Chaudhry & Aditi Sharma, *India: How IP protection has improved this year*, MANAGING INTELL. PROP., October 2009: Supplement – Asia-Pacific & Middle East IP Focus 2009 (7th ed.), *available at* http://www.managingip.com/Article.aspx?ArticleID=2311540.

[101] Lex Orbis Intellectual Property Resource Centre – Lack of "enhanced efficacy" and High Price deprives Glivec of a Patent, http://www.lexorbis.com/Lack_of_enhanced_efficacy.htm (last visited July 8, 2010).

[102] Lex Orbis Intellectual Property Resource Centre – Mashelkar Committee Report accepted by the Government, http://www.lexorbis.com/Mashelkar_Committee_Report_accepted_by_the_Government.html (last visited July 8, 2010).

the possibility to register essentially derived varieties.[103] On the other hand, the legislation attempts to balance in a rather unique manner the rights of commercial breeders and those of traditional small-scale and subsistence farmers. The conflicting goals come to expression in the preamble of the Act. On one hand, it speaks of the necessity "to recognize and protect the rights of farmers in respect of their contribution made at any time in conserving, improving and making available plant genetic resources for the development of new plant varieties", while on the other hand it regards plant breeders' rights protection as a necessary precondition "for accelerated agricultural development" and "to stimulate investment for research and development" as well as to "facilitate the growth of the seed industry."

Farmers' rights are regulated in Chapter VI of the legislation. Interestingly, and going beyond schemes for mere compensation of traditional contributions, the PPVFRA allows for the registration not only of new and essentially derived varieties, but also of "farmers' varieties" as well as of so-called "extant varieties." The definitions of these varieties can be collected from section 2. A "farmers' variety" is defined in section 2(l) of the PPVFRA as "a variety which: (i) has been traditionally cultivated and evolved by the farmers in their fields; or (ii) is a wild relative or land race of a variety about which the farmers possess the common knowledge". Farmers' rights are once again mentioned as a sub-category of "extant variety", which according to section 2(j) is a variety notified under section 5 of the Seeds Act, a farmers' variety, a variety about which there is common knowledge, or any other variety which is in the public domain. "Extant varieties" are, therefore, varieties recognised or in existence at the time of the coming into force. The PPVFRA allows for registration of extant varieties and of farmers' varieties (section 14 (b) and (c), PPVFRA), which, in the case of farmers' varieties, can be effected by "any farmer or group of farmers or community of farmers claiming to be the breeder of the variety" (section 16 (d), PPVFRA). While the registration requirements for new varieties are novelty, distinctiveness, uniformity and stability (section 15(1)), novelty has been dispensed with in the case of extant varieties, which need to conform only to "such criteria of distinctiveness, uniformity and stability as shall be specified under regulations made by the Authority" (section 15(2)). Of course, "a famer who has bred or developed a new variety shall be entitled for registration and other protection in like manner as a breeder of a variety under this Act." However, farmers' varieties are of course not new, but as a sub-group of extant varieties they still have to conform to the distinctiveness, uniformity and

[103] *See* § 23, Protection of Plant Varieties and Farmers' Rights Act, 2001, No. 53 of 2001 (PPVFRA); *see also supra* note 90, at 219; *see also* S. K. Verma, *Protection of Traditional Knowledge in the SAARC Region and India's Efforts*, *in* TRADTIONAL KNOWLEDGE, TRADITIONAL CULTURAL EXPRESSIONS AND INTELLECTUAL PROPERTY LAW IN THE ASIA-PACIFIC REGION 315, 330 (Christoph Antons ed., 2009).

stability (DUS) criteria. Critics have, therefore, concluded that the extent to which farmers will be able to make use of the registration option may remain quite limited.[104] First statistical figures discussed below seem to confirm that this is a justified concern.

Different from established forms of intellectual property rights, the legislation does not provide some form of royalties enforceable by the farmers against other private parties. Instead, farmers "shall be entitled in the prescribed manner for recognition and reward from the National Gene Fund" (section 39(1)(iii), PPVFRA).[105] The National Gene Fund is constituted by the Central Government. Credited to this National Gene Fund are benefit-sharing payments, annual fees paid to the authorities, money received from compensation claims and contributions to the fund from national and international organisations and other sources (section 45(1)(a)-(d), PPVFRA). Rather than benefit sharing agreements freely negotiated between the users and the breeders of the farmers' varieties, the legislation foresees a determination of the benefit sharing by a government authority, the Protection of Plant Varieties and Farmers' Rights Authority (hereinafter 'Authority').

The Authority is regulated in Chapter II of the PPVFRA. It is the main government agency responsible for plant variety protection and for the registration of the various varieties. Its composition is prescribed in section 3 (5), PPVFRA. It was being established from the end of 2005 with the appointment of the Plant Varieties Protection and Farmers' Rights Board.[106] The notification of the Protection of Plant Varieties and Farmers' Rights Regulations followed in December 2006. In 2007, the Authority began to publish the Plant Variety Journal of India as well as guidelines for the conduct of the Distinctness, Uniformity and Stability (DUS) testing. Initially, guidelines for twelve crops were published. According to the website of the Authority,[107] registration is now open for 31 crop species.

Statistics on the website of the Authority also indicate that extant varieties other than farmers' varieties thus far account for the bulk of the Authority's work. This was anticipated in the Protection of Plant Varieties and Farmers' Rights Regulations of 2006, which in Rule 6 prescribed

---

[104] *Supra* note 94, at 149; Verma, *id.* at 331.
[105] Verma, *supra* note 103, at 330-331.
[106] *Farmers hail PVP & FR Act notification*, FIN. EXPRESS, Nov. 14, 2005, *available at* http://www.financialexpress.com/news/Farmers%20hail%20PVP%20&%20FR%20Act%20notification%20%20/159181/.
[107] *See* Protection of Plant Varieties and Farmers' Rights Authority, India – Registration Open For, http://www.plantauthority.gov.in (last visited July 8, 2010).

the constitution of an Extant Variety Recommendation Committee (EVRC). About 40 extant varieties covering nine crop species have been registered in 2008-2009.[108] Section 28(1) PPVFRA confirms the essentially public character of many of the "extant varieties" notified under the Seeds Act of 1966 when seed production was still largely seen as a task for the public sector. In the case of an extant variety, "unless a breeder or his successor establishes his right", the Central Government or the State Government, where notification occurred for a state, shall be deemed to be the owner of such right. The 1003 applications for registrations of extant varieties contrast with 353 applications for new varieties, which are now under examination or DUS testing. Eighteen applications for farmers' varieties are equally under examination.

Where there is an entitlement for recognition and reward from the National Gene Fund, the Authority fixes the amount of benefit sharing after giving the parties the opportunity to be heard by taking into consideration the extent and nature of the use of genetic material of the claimant in the development of the variety and the commercial utility of and market demand for the variety (section 26, PPVFRA).

Apart from such benefit sharing claims of individual or collective breeders of traditional varieties, there is further under the heading "rights of communities" in section 41, PPVFRA a right to lodge a compensation claim against a commercial breeder for the contributions of a community to the evolution of a variety used in the breeding process. This claim may be raised by any person, group of persons (whether actively engaged in farming or not) or any governmental or non-governmental organisation on behalf of any village or local community in India. The decision whether or not to grant compensation and the amount of compensation is again a discretionary decision of the Authority. Commentators have raised concerns about the partly overlapping and partly diverging regulations on benefit sharing and compensation in the legislation, which may give rise to confusion and disputes. Equally, the lack of real property rights and the dependence on the Authority in the current scheme have been criticised.[109] In particular, it has been observed that the effect of the current legislation is that breeders may have to pay more than once for using traditional knowledge, because of the overlap between benefit sharing and compensation to the community. At the same time, commentators have found a "reluctance of Parliament to recognize that ownership of traditional knowledge rests with the community and to develop legislation from that perspective", so that "it can safely be concluded that the provisions to protect the traditional

[108] PROTECTION OF PLANT VARIETIES AND FARMERS' RIGHTS AUTHORITY, ANNUAL REPORT 2008-2009 (2009), *available at* http://plantauthority.gov.in/pdf/AnnualReport_08-09esum.pdf.
[109] *Supra* note 90, at 220.

knowledge of the farming community are not going to work to the advantage of these communities."[110]

Apart from the benefit sharing and compensation mechanism, section 39(1)(iv), PPVFRA also provides for the traditional farmers' right to reuse saved seed, including to exchange, share or sell it. Here, however, the legislation follows the 1991 UPOV model in that the farmer is not allowed to sell branded seed of a protected variety.

Section 39(2), PPVFRA allows for a further compensation claim by farmers against commercial breeders on the grounds that the performance of a commercial variety remains below the performance projections that the commercial breeder had disclosed in advance. Again, the Authority will make the decision about such compensation after hearing the parties. Finally, commercial breeders need to disclose and acknowledge the contribution of traditional breeders in their applications. Failure to do so will result in a rejection of the application (section 40, PPVFRA).

3. The Biological Diversity Act

The Biological Diversity Act, 2002 constitutes India's implementation of the provisions of the CBD. In its preamble, the Act reaffirms the sovereign rights of states over their biological resources and explains that it wants to provide for conservation, sustainable utilisation and equitable sharing of benefits arising out of the utilisation of genetic resources. The Act creates yet another string of state agencies responsible for permits, guidelines and the supervision of the implementation of the Act. These agencies are the National Biodiversity Authority (NBA), the various State Biodiversity Boards (SBB) and, at the local level, Biodiversity Management Committees (BMC), constituted by *panchayats*[111] and municipalities. The NBA is largely an inter-ministerial committee with a number of non-official members to be appointed from the scientific community, industry representatives, conservers, creators and knowledge holders (section 8). One of the sub-committees of the NBA may deal with agro-biodiversity, defined as biological diversity of agriculture related species and

---

[110] N. S. Gopalakrishnan, *Protection of Traditional Knowledge: The Need for a Sui Generis Law in India*, 5 J. WORLD INTELL. PROP. 725, 735 (2002).

[111] 'Panchayats' is a term widely used in India for dispute resolution institutions that can be caste based, territory or village based, or tribe based. For details, *see* Upendra Baxi, *People's Law in India – The Hindu Society*, *in* ASIAN INDIGENOUS LAW: IN INTERACTION WITH RECEIVED LAW 216, 234-256 (Masaji Chiba ed., 1986). The panchayat system finds constitutional recognition in Part IX of the Indian Constitution, where panchayats are referred to as democratic institutions of self-government for rural areas with specific responsibilities for economic development and social justice at the local level.

their wild relatives (section 13(1)). Responsibilities of the NBA important in this context relate in particular to the approval of activities under sections 3, 4 and 6 of the Act, dealing with access to biological resources and associated knowledge; transfer of research results; and acquisition of intellectual property rights (section 18(2)). The NBA further issues regulations and guidelines for these matters (section 18(2)). It has an advisory role to central and state governments and an important role in opposing the granting of intellectual property rights on Indian biological resources or associated knowledge outside of India (section 18(3) and (4)).

State Biodiversity Boards are also inter-departmental committees with additional members drawn from experts on biodiversity and sustainability. Biodiversity Management Committees at the local level are constituted to promote conservation, sustainable use and documentation of biological diversity including preservation of habitats, conservation of land races, folk varieties and cultivars, domesticated stock and breeds of animals and microorganisms, and chronicling of knowledge relating to biological diversity. They are only to be consulted by the other bodies in their decision making processes, although they may levy fees and charges for biological resources collected within their areas (section 41).

The Act has further been supplemented with the Biological Diversity Rules issued in 2004. Much to the disappointment of local activists and NGOs favouring decentralised decision-making and administration,[112] the Rules confirmed the central role of the Authority in decisions about access, knowledge transfer and intellectual property rights. According to Rule 14, it is the Authority that enters into an agreement regarding access with an applicant "after consultation with the concerned local bodies" and it is in the Authority's discretion to impose conditions, including the quantum of monetary and other incidental benefits, restrictions (Rule 16) or to revoke an approval under certain conditions (Rule 15). Local activists had hoped for a stronger role for the local Biodiversity Management Committees, whose role remained confined, however, to the collection of data for the so-called People's Biodiversity Registers and to the giving of advice to the Authority and State Biodiversity Boards during the granting of approvals (Rule 22). In 2007, *panchayats* and community representatives submitted over 3000 resolutions to the Prime Minister expressing their concerns over the reduced role of the Biodiversity Management Committees.[113]

---

[112] *Biodiversity Act, Rules opposed*, HINDU, Dec. 8, 2004, *available at* http://www.hinduonnet.com/2004/12/08/stories/2004120815390300.htm.

[113] *The bio-diversity Act is progressive, but not fool-proof*, FIN. EXPRESS, Apr. 30, 2007, *available at* http://www.financialexpress.com/news/The%20bio-diversity%20Act%20is%20progressive,%20but%20not%20fool-proof/106130/.

The Act develops rules for access to biological resources and associated knowledge by distinguishing between resident Indian nationals, on the one hand, and foreigners, foreign corporations or corporations with foreign shareholding or under foreign management, foreign residents and Indian non-residents on the other hand. The latter groupings require the approval of the National Biodiversity Authority to obtain biological resources occurring in India or associated knowledge for research or commercialisation or for bio-survey and utilisation (section 3). It is equally prohibited without approval of the NBA to transfer research results to foreigners or foreign residents, with certain exceptions for academic purposes and for certain collaborative research projects to be outlined in Central Government guidelines (sections 4 and 5).[114] The relevant guidelines for such collaborative projects have meanwhile been notified.[115] Importantly, the approval of the NBA is further required for any acquisition of intellectual property rights in or outside India, if the invention is based on research or information on a biological resource obtained from India. For patents, this is mitigated by the fact that the permission must be obtained before the sealing of the patent, but may come after acceptance of the patent by the patent authority (section 6(1)). Exempted are further applications for plant varieties regulated under the Plant Varieties Act (section 6(3)). The section provides the opportunity for the NBA to impose benefit sharing fees or royalties or conditions (section 6(2)).

The NBA largely determines any benefit-sharing conditions in accordance with mutually agreed terms and conditions between the applicants and local bodies concerned and benefit claimants (section 21(1)). While this implies a wide-ranging recognition of individually negotiated conditions, Rule 20 of the Biological Diversity Rules explains that "the quantum of benefits shall be mutually agreed upon between the persons applying for such approval and the Authority in consultation with local bodies and benefit claimers" (Rule 20(5)).

The BDA and the Rules empower the Authority also to impose far-reaching conditions, including the granting of joint ownership in intellectual property rights to the NBA itself or to the benefit claimants, technology transfer, requests for production or research and development (R&D) units in areas of the benefit claimants, the involvement of Indian scientists, benefit claimants and local people in R&D activities, the setting up of a venture capital fund for the benefit claimants or the payment of monetary compensation or non-monetary benefits to such claimants at the discretion

[114] Verma, *supra* note 103, at 333.

[115] National Biodiversity Authority, India - Notifications, http://www.nbaindia.org/notification.htm (last visited July 8, 2010). For an earlier critical expression of concerns over the effects of the Act on biodiversity research, *see also* K. D. Prathapan et al., *Biological Diversity Act 2002: Shadow of permit-raj over research*, 91 CURRENT SCI. 1006 (2006).

of the NBA (section 21(2)). The formula for benefit-sharing shall be determined on a case-by-case basis and notified in the Official Gazette (Rule 20(1) and (3)). If the compensation or benefit sharing is paid in money, the NBA may direct these funds to individuals, groups or organisations that can be identified as the source of the resource or knowledge. If that is not possible, the benefits shall be deposited in the National Biodiversity Fund (section 21 (3), BDA, Rule 20(8), Biological Diversity Rules).

Indian citizens or corporations are treated differently under section 7. Indian citizens and corporations must give prior intimation to their relevant State Biodiversity Board to obtain biological resources for commercial utilisation or bio-survey and bio-utilisation. For local people and communities of the relevant area, growers and cultivators of biodiversity and for practitioners of indigenous medicine, even this requirement will be dispensed with. The SBBs are responsible for the granting of approval, where necessary, to Indian citizens for commercial utilisation or bio-survey/bio-utilisation and they also fulfil an advisory role to the state governments (section 23). For activities, which require only intimation to the SBB, the SBB may at its discretion prohibit or restrict such activities if it regards them as detrimental or contrary to the objectives of conservation and sustainable use of biodiversity or to the equitable sharing of benefits (section 24(2)). In other words, while commercial activities of foreigners are prohibited unless specifically approved, those of resident Indian nationals are mostly allowed unless specifically prohibited. It appears from sections 19(2) and 20(1), however, that even Indians must get approval to acquire intellectual property rights related to the resources/knowledge or to transfer such knowledge abroad.

The Act creates biodiversity funds at national, state and local levels for administration of benefits to claimants and community benefits, conservation purposes and management of heritage site. Some of the funds, however, may also be used for purposes of socio-economic development and to meet expenses incurred (sections 27, 32 and 44, BDA, Rule 20(9) Biological Diversity Rules). Under section 40, the Central Government after consultation with the Authority is empowered to exempt any items, including biological resources normally traded as commodities, from the provisions of the Act. The Act contains penalties for contraventions of the provisions governing access, knowledge transfer, acquisition of intellectual property rights and intimation to the SBB.

Apart from the concerns of local activists mentioned above, the Indian Biodiversity Act has also attracted criticism in the academic literature. First, the very lenient treatment of Indian citizens and especially companies and the limitations to knowledge holders vis-à-vis these local interests has

been noted.[116] Second, it has been noted that about 40 per cent of the world-wide accessions for food crops are in the collections of the Consultative Group for International Agricultural Research (CGIAR) and India is itself highly dependent on access to these resources and to resources from other regions.[117] Third, because of a lack of extraterritorial authority, the NBA cannot effectively monitor applications outside India[118] and it would neither have the time nor the resources to challenge patents in many foreign jurisdictions.[119] Fourth, the relationship between the discretionary decisions of the NBA on benefit-sharing and the agreements reached between applicants and knowledge holders remains unclear as does the relationship between the NBA and SBBs and the BMCs.[120] Fifth, local communities have not automatic right to the benefits, but depend on the direction of the funds by the authorities.[121] Sixth, benefit sharing and the formula for it needs fine tuning and the possibility of joint IP ownership as stipulated in section 21, BDA may hardly be acceptable to multinational companies.[122] Seventh, the legislation promotes a strong property rights framework under central control with little regard to common property arrangements.[123] And eighth, in spite of attempts to avoid overlaps with the plant varieties legislation, there clearly is such an overlap with regard to agro-biodiversity and related benefit-sharing decision making.[124] One commentator concluded, therefore, that the Act "in practice does not provide effective measures for protection of biological resources and is heavily biased against the interests of tribal and local communities who are the guardians of associated knowledge."[125] The lenient provisions for Indian nationals and especially for Indian industry "even seem to encourage commercial exploitation of resources rather than giving impetus to the conservation of biodiversity or to benefit-sharing with the local communities."[126]

---

[116] *Supra* note 90, at 216; *see also* Rajesh Sagar, *Intellectual Property, Benefit-Sharing and Traditional Knowledge: How Effective is the Indian Biological Diversity Act, 2002?*, 8 J. WORLD INTELL. PROP. 383, 387-388 (2005); *see also supra* note 110, at 740; *see also* Verma, *supra* note 103, at 337-338 (in relation to the controversial benefit-sharing arrangements for the drug 'Jeevani' based on traditional knowledge provided by the Kani tribe of Kerala).

[117] *Supra* note 90, at 216.

[118] Verma, *supra* note 103, at 334.

[119] *Supra* note 90, at 217 & 225; Sagar, *supra* note 116, at 391.

[120] *Supra* note 110, at 738.

[121] *Supra* note 90, at 218; *see also supra* note 110, at 739; *see also* Verma, *supra* note 103, at 335.

[122] Verma, *supra* note 103, at 335.

[123] *Supra* note 90, at 218; however, note the critical discussion of community intellectual property rights in Verma, *supra* note 103, at 335.

[124] Sagar, *supra* note 116, at 386-387; *see also* Verma, *supra* note 103, at 335; *see also* Ranjan, *supra* note 50, at 229.

[125] Sagar, *supra* note 116, at 400; *see also Changes in Bio-Diversity Act sought*, HINDU, Dec. 30, 2004, *available at* http://www.hinduonnet.com/2004/12/30/stories/2004123015730300.htm (appeal from over 200 panchayats and several NGOs to strengthen community control over bio-diversity).

[126] *Id.*

After the enactment of the BDA in February 2003, it took until 2005 until the necessary expert committees were formed and procedural guidelines were drafted.[127] Meanwhile, the NBA has drafted and published on its website the application forms and standard agreements for access to biological resources and/or associated knowledge for commercial utilization, access for research/bio-survey and bio-utilisation, seeking intellectual property rights, transfer of research results and for third party transfer of bio-resources and/or associated knowledge.[128] According to statistics on its website, the NBA approved from January 2006 to August 2008 twenty-four access applications, transfer of nine research results applications, two-hundred-and-sixty-six intellectual property rights applications, sixteen third party transfers and forty collaborative research projects under section 5, BDA. The agreement between NBA and the applicants has been signed for thirteen access applications, transfer of eight research results applications, thirty-three intellectual property rights applications and fourteen third-party transfer applications.[129]

The Government of India is also undertaking major efforts to establish biodiversity registries and digital libraries to prevent patenting of Indian traditional knowledge abroad. These include the People's Biodiversity Registers, which are an important task for the Biodiversity Management Committees, and the Traditional Knowledge Digital (TKDL), which is currently focused on traditional medicine and medicinal plants.[130] The TKDL has been translated into English, Spanish, German, French and Japanese and under a three-year agreement made available to patent examiners at the European Patent Office to assist with their prior art searches. Reportedly, prior art ascertained on the basis of the TKDL already prevented the patenting of a melon extract formulation, which is a traditional Indian method of treatment, for the treatment of leucoderma. The short period of only three weeks was contrasted favourably with the ten years it took Indian authorities to challenge the patents on neem and turmeric.[131] It has also been reported that other developing countries wish to build similar databases and seek assistance from India.[132]

---

[127] *Looking after India's biodiversity*, MANAGING INTELL. PROP., July-August 2005: Supplement – India IP Focus 2005, *available at* http://www.managingip.com/Article.aspx?ArticleID=1321448 (interview with K. Venkataraman – secretary to the National Biodiversity Authority, India).

[128] National Biodiversity Authority, India – Applications, http://www.nbaindia.org/applications/application.htm (last visited July 8, 2010); National Biodiversity Authority, India – Approvals, http://www.nbaindia.org/approvals.htm (last visited July 8, 2010).

[129] National Biodiversity Authority, India – Status of Applications, http://www.nbaindia.org/approvals/status_approvals.htm (last visited July 8, 2010).

[130] *See* Verma, *supra* note 103, at 336.

[131] Lex Orbis Intellectual Property Resource Centre – India Successfully Blocks Spanish patent on its Traditional Knowledge, http://www.lexorbis.com/India_Successfully_Blocks_Spanish_patent_on_its_Traditional_Knowledge.html

4. The Seeds Bill

In 2004, the Indian Government introduced a new Seeds Bill to replace the Seeds Act of 1966. Since then it has generated much controversy. Government statements on the website of the Department of Agriculture and Cooperation explained the reasons for the new law. Among the more important reasons is the creation of a facilitative climate for growth of the seed industry, boosting of the export of seeds and encouragement of the import of useful germplasm and the creation of a conducive atmosphere for application of frontier sciences in varietal development and for enhanced investment in research and development.[133] The latter reason refers especially to transgenic varieties, which are now included in the draft. The government points out that GM seeds are generally not notified under the previous Act. As the seeds are very costly and farmers have sometimes been cheated, there is a need for regulation and strengthening of testing and seed testing laboratories involved.[134] The draft seeks to achieve this by widening the circle of institutions accredited to conduct agronomic trials and testing, which, besides public centres and universities, would also include private organisations and private seed testing laboratories.

Whereas under the current legislation only notified varieties have to be registered, all seeds for sale must be registered under the Seeds Bill. The Bill foresees Central and State Seed Committees as well as a Registration Sub-Committee to keep a National Register of Seeds. There are provisions for transgenic varieties and for fines and imprisonment for contravention of the Act and for providing false information.[135]

Critics of the bill argue that traditional and small-scale farmers should be concerned in particular that it regulates not only the selling, keeping for sale, offering to sell, import or export of seed, but mentions in the same context also bartering, a typical manner of seed exchange among traditional farmers.[136] This, it is argued, has the potential to further limit the avenues for exchange of seeds.[137]

(last visted July 8, 2010).

[132] Lex Orbis Intellectual Property Resource Centre – MoU between India and US on IPR Protection, http://www.lexorbis.com/MoU_between_India_and_US_on_IPR_Protection.htm (last visited July 8, 2010).

[133] New Policies Initiation In Seed Sector – New Seeds Bill (Apr. 1, 2005), http://agricoop.nic.in/PolicyIncentives/NewSeedBill.htm (last visited July 8, 2010).

[134] New Policies Initiation In Seed Sector – Use of Biotechnology in Agriculture (Apr. 1, 2005), http://www.agricoop.nic.in/PolicyIncentives/UseOfBiotechnology.htm (last visited July 8, 2010).

[135] For a detailed comparison between the provisions of the Bill and the 1966 Seeds Act, *see* M. R. MADHAVAN & KAUSHIKI SANYAL, LEGISLATIVE BRIEF: THE SEEDS BILL, 2004 (2006), *available at* http://www.prsindia.org/uploads/media/1167468389/legis1167477737_legislative_brief_seeds_bill.pdf.

[136] *See, e.g.*, §§ 22(1), 25, 28(1), 38(b), 38(c), 38(d), Seeds Bill, 2004.

[137] Shiva, *supra* note 93.

The Bill has further been criticised for its potential contradictions to and undermining of the provisions of the Protection of Plant Varieties and Farmers' Rights Act.[138] For while the Seed Bill confirms the farmers' privilege that "nothing shall restrict the right of the farmer to save, use, exchange, share or sell his farm seeds and planting material", this comes with the restriction "except that he shall not sell such seed or planting material under a brand name or which does not conform to the minimum limit of germination, physical purity, genetic purity prescribed…". Critics point out that this could make farmers anxious about small local sales in village sales and could prevent the registration of their traditional varieties, which may not pass the required standards.[139] While the Bill is concerned with compensation for farmers if commercial seeds do not perform to expected levels, it refers potential claimants to the Consumer Protection Act of 1986.[140] However, this is a less straightforward avenue than under similar compensation provisions in the PPVFRA, in which the Protection of Plant Varieties and Farmers' Rights authority assesses the case and grants the compensation. This latter avenue would seem far preferable, particularly as the urban based consumer courts are not very accessible for farmers in rural areas.[141] Observers in the Indian media concluded, therefore, with regards to the Seeds Bill, 2004 that "public interest demands that its legal incongruities and farmer-unfriendly provisions are corrected before the Seeds Bill is passed by Parliament."[142] The discussion may soon be back in Parliament, as the government is expected to table in the next session a report from the Parliamentary standing committee on agriculture on the Seeds Bill.[143]

5. The Protection, Conservation and Effective Management of Traditional Knowledge Relating to Biological Diversity Rules, 2009

In early 2010, the NBA released a number of draft amendments and requested public comments, including on the Protection, Conservation and Effective Management of Traditional Knowledge

---

[138] Bala Ravi, *Seeds of Trouble*, HINDU, Mar. 8, 2005, *available at* http://www.hinduonnet.com/thehindu/2005/03/08/stories/2005030801761000.htm.

[139] GRAIN & Devinder Sharma, *India's new Seed Bill*, SEEDLING, July 2005, *available at* http://www.grain.org/seedling_files/seed-05-07-5.pdf.

[140] *See supra* note 135; *see also* Shiva, *supra* note 93; *see also id.*

[141] *See supra* note 138.

[142] *See supra* note 138.

[143] *MNCs will dominate if Seeds Bill adopted: Farmers Associations*, BUS. STANDARD, June 29, 2009, *available at* http://www.business-standard.com/india/news/mncs-will-dominate-if-seeds-bill-adopted-farmers-associations/65912/on; Bhavdeep Kang, Why the US is so keen to sell Bt brinjal to India (Nov. 19, 2009), http://business.rediff.com/column/2009/nov/19/why-the-us-is-so-keen-to-sell-bt-brinjal-to-india.htm (last visited July 7, 2010).

Relating to Biological Diversity Rules (subsequently Traditional Knowledge Rules).[144] Commentators are intrigued that this *sui generis* legislation for traditional knowledge protection is not introduced as a Bill and as such subjected to parliamentary scrutiny, but as delegated legislation in the form of rules under the Biological Diversity Act of 2002. Given the broad scope of some of the provisions, the question has been raised whether this is constitutional.[145] The Traditional Knowledge provisions go significantly beyond and frequently contradict those of the Biological Diversity Act. The NBA has just collected public reactions to the Traditional Knowledge Rules. These reactions were collected jointly with those related to the further debates on an international regime on access and benefit sharing and on amendments to the Biological Diversity Act, 2002, and the Biological Diversity Rules, 2004. Since the parent legislation for the Traditional Knowledge Rules could also be amended, it is unclear at this stage how these various laws and rules will ultimately relate to each other and which form the Traditional Knowledge Rules will finally take. Nevertheless, a few preliminary comments can be offered. First, it is interesting to note that the Rules apply a very wide definition of 'traditional knowledge', which includes traditional cultural expressions. Thus, 'traditional knowledge' relates not only to "properties, uses and characteristics of plant and animal genetic resources; agriculture and healthcare practices, food preservation and processing techniques and devices developed from traditional materials", but also to "cultural expressions, products and practices such as weaving patterns, colours, dyes, pottery, painting, poetry, folklore, dance and music." Equally wide is the definition of beneficiaries belonging to a 'traditional community', which includes "families, people belonging to Scheduled Tribes as per Article 342 of the Constitution of India, and other notified tribal groups including nomadic tribes…" The inclusion of families shows that tradition is, quite rightly, not supposed to remain confined to tribal groups. However, in view of the definition of 'misuse of traditional knowledge' as "access to and/or use of traditional knowledge by persons not belonging to the traditional community" without license or in breach of licensing terms, it brings back the question how group/community membership is defined and who decides about membership. This is all the more important, because the Traditional Knowledge Rules differ from the regulations in the Biodiversity Act in that they provide for direct negotiations between a user (or 'accessor' in the terminology of the Rules) and a traditional community and for direct payment of the benefits to the traditional community.

---

[144] Prashant Reddy, The National Biodiversity Authority invites comments on draft amendments (Feb. 2, 2010), http://spicyipindia.blogspot.com/2010/02/national-biodiversity-authority-invites.html (last visited July 7, 2010).

[145] Prashant Reddy, A Comment on the Vires of 'The Protection, Conservation and Effective Management of Traditional Knowledge relating to Biological Diversity Rules, 2009' (Feb. 15, 2010), http://spicyipindia.blogspot.com/2010/02/comment-on-vires-of-protection.html (last visited July 7, 2010).

While the Rules in so far strengthen the role of the communities, the national and state authorities still have the final say in many instances, for example, if traditional knowledge is already in the public domain, not specifically owned by any particular community or is owned by communities spread out over more than three states. It gives the NBA decision-making powers over access by one traditional community to the knowledge of another community, if this is for earning their livelihood and not for commercial gain. It requires from communities to comply with the registration requirements of the Traditional Knowledge Register, if they want to receive benefits. Users, on the other hand, have to await the outcome of fairly complicated and potentially lengthy procedures, involving national and state authorities as well as local communities, to finally get access. These procedures include a potential waiting period of up to one year to allow states to set up State Biodiversity Boards and/or Biodiversity Management Committees, where they do not yet exist. Assessment further involves a report by such committees on such complicated matters as sustainability of resources, social and environmental implications and potential value of the knowledge as well as a resource management plan.

VIII

CONCLUSION

The last few decades have seen a shift from an understanding of agricultural and biological resources as the "common heritage of mankind" to an understanding where such resources are under the sovereign control of nation states. This has been accompanied by a strengthening of the intellectual property rights system for biological material in the wake of the WTO-TRIPS Agreement and more recently on the basis of bilateral Free Trade Agreements between developed and developing nations. The result has been a further shift in the agricultural sector of developing countries from public research institutions to private R&D. Under the circumstances, traditional knowledge and farmers' rights are defended as a crucial counterweight in societies that are still dependent on the farming sector.[146]

The debate about traditional knowledge protection links up to a larger debate about approaches to the environment and to sustainable development in developing countries. Here, the failure of statist planning has led to a move away from top-down solutions to development and to environmental management and to a search for bottom-up approaches. At first, these were mainly

[146] Shiva, *supra* note 93; Janak Rana Ghose, *The Right to Save Seed* (Int'l Dev. Research Ctr., Rural Poverty and Environment Working Paper Series – Working Paper No. 13, 2003), *available at* http://www.idrc.ca/uploads/user-S/11205983131The_Right_To_Save_Seed.pdf.

seen in the form of privatisation and private monopoly rights, but more recently there is also a renewed interest in limited common property rights of communities and in a revitalisation of customary law systems.[147]

This article has examined two examples from Asia for attempts to implement a system for traditional knowledge protection using a variety of intellectual property and *sui generis* mechanisms. However, there is a significant difference in the approaches used in the Philippines on the one hand and in India on the other hand. The Philippines case study presents an attempt at a bottom-up approach focusing on the country's indigenous communities. Because the country inherited US administrative models for indigenous communities, it is the only country in East and Southeast Asia that appears not dissimilar in its approach to the settler societies of North and South America, Australia or New Zealand. Its legislation for the protection of indigenous peoples' rights and its regulations for access to biological resources were also the first in this part of Asia and, at the time, widely praised as model solutions. At the time the Philippines government departed from an ecological perspective inspired by the Rio Earth Summit. Subsequent developments, however, did not live up to the high hopes that the initial legislative measures had generated. For example, while the Indigenous Peoples' Rights Act gives recognition to 'community intellectual rights', their concrete implementation has been lacking. Because of its link to issues of indigenous self-determination and land claims, the legislation soon came under pressure from powerful mining interests. Further, the holistic understanding of 'community intellectual rights' did not lend itself to any concrete implementation in the form of mainstream intellectual property laws. What remains is a centrally administered bio prospecting and access legislation safeguarding the need for prior informed consent from and benefit-sharing with indigenous communities as far as their areas are concerned. The results thus far have been disappointing, because no applications were submitted since the bio prospecting rules were revised in 2005 indicating that their stricter conditions may scare off potential applicants.

In contrast to the Philippines, India has from the outset taken a much more centralist approach to traditional knowledge. India belongs to a group of countries that have resisted attempts by international organisations to focus on 'indigenous people' and prefers to speak of 'local and indigenous communities.' Not surprisingly then, and also in view of the differences in economic structure between India and the Philippines, the focus of the debate in India is on agricultural biodiversity and on farming, with farmers' rights featuring particularly prominently in the

[147] *See, e.g., supra* note 53, at 245 & 338.

Protection of Plant Varieties and Farmers' Rights Act. While this Act allows for the registration of farmers' varieties, it falls short of establishing a real property right of farmers to their knowledge and instead makes them dependent on the national authority for most benefit sharing and compensation claims. Confirming the nationalist and centralist approach further, the Biological Diversity Act distinguishes sharply between foreign and Indian national access to biological resources and leaves local communities with little protection against the latter group of users and with little immediate influence in negotiations about benefit-sharing. This would change to some extent, if the Traditional Knowledge Rules drafted under the Biodiversity Act in 2009 and currently presented for public discussion would find approval. The Rules decentralise the negotiation process over access and benefit sharing and strengthen in so far the role of communities. Otherwise, however, national and state authorities retain a central role and the procedures are overall quite complicated and bureaucratic, which in the end could put off potential users and traditional communities alike from using the system.

Developing countries seem torn between a desire to develop high tech and biotechnology industries and a need to look after the interests of a large traditional farming sector. It is in this latter context that traditional knowledge has received great significance and raised hopes that so far have rarely been justified by the relatively meagre benefits. In fact, traditional knowledge may only assist in safeguarding the traditional farming sector or biodiversity, if it is accompanied by policy decisions that go far beyond the relatively narrow field of intellectual property. It seems further important that the focus is redirected towards the original conservationist goals of the CBD. Thus, if royalties for the use of traditional knowledge are collected at the national or state level, then it is important that such benefits are passed on to those communities at the grassroots level that are regarded as the most important stakeholders in the new 'bottom up' environmental protection models. It is further important to gain a realistic understanding of the expectations of users and those who are seeking access, so that access regulations do not become overly complicated and unwieldy for users and knowledge holders alike. The traditional knowledge discussion has certainly sensitised IP academics and practitioners to imbalances in the system that require correction. The successful prevention of a traditional knowledge based patent with prior art information from the Indian TKDL shows that this adjustment process is making progress.

Beyond this, the traditional knowledge debate has put intellectual property into an unfamiliar environment where it is no longer concerned with clearly delineated territorial rights in the modern sector of nation states. The debate takes place at the grassroots level, it involves local

development plans as well as communities and their customary laws and it is messy and intensely political. Here, in discussions about decentralisation, environmental problems and new development paradigms, new rights discourses emerge that use elements from customary law and from different traditions. In how far all of this will affect intellectual property law remains to be seen, but as increasingly influential developing countries decentralise, intellectual property will to some extent have to adjust or risk to become marginalised outside of the commercial enclaves of big cities.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 6, 2010

BEYOND COPYRIGHT: POSSIBLE SOLUTIONS TO AN INTERNET GOVERNANCE REGIME

Meera Jayakumar & Hemangini Dadwal[*]

I

INTRODUCTION: COPYRIGHT HAS OUTLIVED ITS UTILITY

A long time ago, a brilliant example of man's scientific vision came to light with Charles Darwin's Theory of Natural Selection. Herbert Spencer added clarity to the implications of this theory through the term 'the survival of the fittest.'[1] Charles Darwin propounded that only those organisms will be fit to survive which can adapt to changing environments, i.e., only the most resilient will prevail. Almost a century and a half later, this theory is incredibly relevant to cyberspace also. For, what other phrase would better describe the insignificant withering away of copyright regulations for data spread over the internet?

There has been much debate over the general proposal that IP law should be re-designed to suit the climate of cyberspace.[2] However, in this paper, we propose that the very premise of IP law in general, and copyright in particular, as it stands on its own, is redundant for the regulation of the internet. Consequently, we propose two regulatory solutions that can complement the present copyright law regime through improved control over access to data spread over the internet, viz., the Creative Commons approach and the Tier Model for internet regulation.

The basic argument taken in favour of strong IP protection is that it supports and engenders creative activities.[3] It is true that creative activities typically involve a substantial development cost,[4]

---

[*] Final Year, B.A., LL.B. (Hons.), Gujarat National Law University.

[1] Letter from Charles Darwin, to A. R. Wallace (July 5, 1866) (on file with the Darwin Correspondence Project), *available at* http://www.darwinproject.ac.uk/entry-5145.

[2] Maria L. Montagnani & Maurizio Borghi, *Positive Copyright And Open Content Licences: How To Make A Marriage Work By Empowering Authors To Disseminate Their Creations*, 12 INT'L J. COMM. L. & POL'Y 244 (2008).

[3] Richard A. Posner & William M. Landes, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325 (1989). Over the years, in the United States, as elsewhere, the degree of protection has steadily expanded, from the modest Copyright Act of 1790, which offered 14 years of protection with a renewal period of 14 years, to the legislation passed in 1831 (28 years), 1909 (renewal extended to 28 years), 1976 (50 years after the author's death), 1992 (automatic

and as creators alone incur these high costs, they find it necessary to recoup these costs by restricting access to their work through exclusive financial transactions relying on strong IP protection.[5] Although there is some consensus that most creators and artists are not motivated solely by financial considerations,[6] the fact that royalty and similar earnings are their main source of income is a relevant consideration in this regard.[7] Hence, the argument in favour of strong IP protection is essentially utilitarian,[8] and this is especially true for copyright laws.[9] Thus, debates about copyright are full of subtexts; they are partly about law, partly about profit, partly about access, and partly about who produces what.[10] In a more immediate sense, these debates ask what role our legal system should play in regulating creation, use, and distribution of cultural and intellectual products.[11]

The underlying premise of current copyright protection is that there is a sole creator of a piece of art and that no one else can physically recreate this piece of art due to inherent physical limitations. These physical limitations make it cumbersome for an ordinary person to create a significant number of perfect copies. Due to the same, unauthorized copying is restricted to an acceptable minimum level using prevalent copyright law.[12] Hence, it is apparent that even if I own an original copy of a book, the only way for me to create additional copies of the book is to make photocopies of the book I own – a rather tedious process, and the photocopied book shall evidently not be of the same quality as the original book.

---

renewal), and 1998 (70 years). *See* Felix Oberholzer-Gee & Koleman Strumpf, *File-Sharing and Copyright* (Harvard Bus. Sch., Working Paper No. 9-132, 2009), *available at* http://www.hbs.edu/research/pdf/09-132.pdf.

[4] PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: FROM GUTENBERG TO THE CELESTIAL JUKEBOX 17-20 (2003).

[5] James Bessen & Eric Maskin, *Intellectual Property on the Internet: What's Wrong with Conventional Wisdom?* (Research on Innovation, Working Paper, 2004), *available at* http://www.researchoninnovation.org/iippap2.pdf.

[6] Paul E. Geller, *Inquiry into Justice in Copyright Law: Toward a Core Author's Right*, *in* INTELLECTUAL PROPERTY AND THEORIES OF JUSTICE (Axel Gosseries et al. eds., 2008).

[7] *Supra* note 3.

[8] This is essentially because weaker copyright is unambiguously desirable if it does not lessen the incentives of artists and entertainment companies to produce new works. Weaker property rights can undermine industry profitability if consumers who would have purchased a work obtain a free copy instead. The utilitarian aspect of IP rights arises because lawmakers trade off the increased incentives to create protected works and the higher prices that consumers face when books, movies, and recordings must not be copied freely. Oberholzer-Gee, *supra* note 3.

[9] Severine Dusollier, *Open Source and Copyleft: Authorship Reconsidered?*, 26 COLUM. J. L. & ARTS 281 (2003).

[10] Adrienne Goss, *Codifying a Commons: Copyright, Copyleft, and the Creative Commons Project*, 82 CHI.-KENT L. REV. 963 (2007).

[11] *Id.*

[12] Eric Priest, *Why Emerging Business Models and not Copyright Law are the Key to Monetising Content Online*, *in* COPYRIGHT LAW, DIGITAL CONTENT, AND THE INTERNET IN THE ASIA-PACIFIC (Brian Fitzgerald et al. eds., 2008).

Copyright law operates as a functional solution in a technologically backward environment. However, with the advent of computers and the internet, the physical limitations preventing copying of works have been largely overcome, and granting copyright protection to data over the internet has become somewhat meaningless owing to the ease with which material can be accessed and copied from any corner of the world at literally no cost to the end-user.

There were three developments, according to one author, that changed the prior functional equilibrium: the emergence of optical disc media, the personal computer and the internet.[13] The development of optical disc media ensured that ordinary users could make near-perfect copies of digital works, including music, movies and pictures, and other copyrightable material in the form of CDs and DVDs and distribute them, even for consideration. The proliferation of the personal computer (PC) enabled innumerable unidentifiable ordinary users to access copyrighted works from their living rooms. Access apart, the PC gave rise to the culture of P-2-P sharing,[14] a development that was instrumental in shutting down Napster, one of the biggest file-sharing networks ever created.[15] However the most significant development of all was the emergence of the internet.[16] The power of the internet lies in its basic simplicity.[17] The strong pervasiveness of the internet ended the final physical limitations that ensured the efficacy of traditional copyright law in protecting artistic creations.[18] Hence, the conclusion becomes clear: traditional copyright law became redundant to protect data and creations in the virtual world.

In support of this conclusion, this paper takes into account two determinant factors:

1. the nature of the internet; and
2. the problem of perspective.

---

[13] *Id.*

[14] BIRGITTE ANDERSEN & MARION FRENZ, THE IMPACT OF MUSIC DOWNLOADS AND P2P FILE-SHARING ON THE PURCHASE OF MUSIC: A STUDY FOR INDUSTRY CANADA (2007), *available at* http://www.ic.gc.ca/eic/site/ippd-dppi.nsf/vwapj/IndustryCanadaPaperMay4_2007_en.pdf/$FILE/IndustryCanadaPaperMay4_2007_en.pdf.

[15] *Supra* note 12.

[16] *Supra* note 12.

[17] Michael Carroll, *Creative Commons as Conversational Copyright*, *in* INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE (Peter K. Yu ed., 2006).

[18] *Supra* note 5.

II

DETERMINANT FACTORS FOR INTERNET GOVERNANCE

The Nature of the Internet

John Gilmore once famously remarked: "The Net interprets censorship as damage and routes around it."[19] Human psychology is such that anything that is prohibited is appealing. In fact, it would not be an exaggeration to contend that prohibition is most often the key to 'negative innovation.'[20] This proposition is also appropriate for cyberspace. To illustrate this point, we don't have to go too far. Most educational institutes forbid access to certain websites on moral grounds. Yet, even students with no exceptional technological capabilities take almost no time in circumventing the embargo to access the blocked websites. The nomenclature of the 'World Wide Web' illustrates adequately the defined scope of the medium, or, more accurately, the lack of a definite scope. The purpose of the internet was global connectivity, enabling virtual accessibility, even if the thing to be accessed were outside physical reach.[21] The internet is a boundless cosmos encompassing several forms of creativity, where what one wants, one gets. It is thus inconceivable that a law that governs the real world can also be used for the virtual one.

The internet carries various information resources and services, such as electronic mail, online chat, movies, file transfer and file sharing, online gaming, and inter-linked hypertext documents and other resources of the World Wide Web (www). The internet is a global data communications system. The internet has made possible new forms of social interaction and activities, owing to its basic features of simple usability and widespread access. Its arrival has brought to the fore a myriad of predictions, controversies, debates and mere conjectures regarding its impact on many facets of modern society. Many others see it as the creator of a new free society, a virtual democracy where information gives people the power to be their best.[22] However, in the final analysis, the internet can be described as an entity that interconnects individual, autonomous computer networks in order to enable such networks to function and appear as one network.[23] Nicholas Negroponte, an

---

[19] Philip Elmer-Dewitt et al., *First Nation in Cyberspace*, TIME INTERNATIONAL, Dec. 6, 1993, *available at* http://www.time.com/time/magazine/article/0,9171,979768,00.html.

[20] This term could refer to such innovation that does not benefit society, that is detrimental to the public good or to the establishment, or that effectively flouts the laws and rules that govern social behaviour and regulate a well-ordered society.

[21] Robert Litan, *Law and Policy in the Age of the Internet* (AEI Center for Regulatory and Market Studies, Working Paper No. 01-04, 2001), *available at* http://reg-markets.org/admin/pdffiles/working_01_04.PDF.

[22] Joseph S. Nye, Jr., *Information Technology and Democratic Governance*, *in* GOVERNANCE.COM: DEMOCRACY IN THE INFORMATION AGE (Elaine C. Kamarck & Joseph S. Nye, Jr. eds., 2002).

[23] MICHAEL A. GALLO & BILL HANCOCK, NETWORKING EXPLAINED 56 (2d ed. 2002).

expert in cyberspace, said about the power of the Net: "In the digital world, the bits are endlessly copy-able, infinitely malleable, and they never go out of print. Millions of people can simultaneously read any digital document- and they can also steal it."[24]

Unlike the traditional concept of IP that envisages a strong cultural image of creative activity as the work of a romantic individual – the artist in the garret or the inventor in the garage, the reality in relation to the internet is quite different. The simple truth is that most creative activity is not the work of single creators. Rather, it is 'interactive' and involves numerous contributions from different parties, who may live in any corner of the earth. Indeed, the process of innovation is often 'sequential', where each creator 'improves' on the work of the previous creator.[25] The traditional concept of IP equates imitation to copying and deems the same to be illegal. However, when innovation is sequential, imitation is more than copying – it adds important value and in turn results in a new work.[26]

In addition, the internet is all-pervasive and omnipresent. The law today prohibits single acts that amount to infringement of copyright entitlements. But technology has developed so much that a single action can result in the infringement of multiple rights of the copyright holder or licensee. It will not be stretching our imagination to say that the law lags behind technology.[27] Something as dynamic as the internet requires something equally potent to keep abreast of its dynamism. The current copyright regime was introduced for protecting publicly available data. Today, this is not a sufficient qualification for a law to govern content available on a medium as extensive as the internet.

In addition, the connectivity objective of the internet has been, to a very large extent, defeated by the imposition of a copyright regime that favours appropriation over accessibility. In other words, a law that restricts accessibility is sought to be applied to a medium that aims to enhance accessibility. The paradox is inescapable. This position is aptly exemplified by John Gilmore's statement – "How many of you have broken no laws this month?"[28]

---

[24] Nicholas Negroponte & Michael Hawley, *A Bill of Writes*, WIRED MAGAZINE, (May 1995), *available at* http://www.wired.com/wired/archive/3.05/negroponte.html.
[25] *Supra* note 5.
[26] *Supra* note 5.
[27] Lyria B. Moses, *Recurring Dilemmas: The Law's Race to Keep Up With Technological Change*, 7 U. ILL. J.L. TECH. & POL'Y 239 (2007).
[28] John Gilmore's homepage (co-founder, Electronic Frontier Foundation, U.S.A.), http://www.toad.com/gnu/ (last visited July 1, 2010).

The Problem of Perspective

We need a protection regime that goes hand-in-glove with the nature of the work and the needs of the creator. Most intellectual property is created and bestowed on the creator or inventor in a uniform manner, with a clear disregard for the type or nature of the work created and the requirements of the creator. Hence, a painter and a writer get identical rights with similar attributes – a copyright. This is true for works on the internet too. This is one of the most important reasons why Creative Commons licensing developed as a concept in the first place. Most creators were not interested in gathering fame or wealth, but created art or writing because they could and they wanted to do so.[29] This evident lack of economic incentives was troublesome, since the rights granted to them restrained them from disseminating their work in any manner they wanted in order to protect supposed economic incentives.

When the internet evolved as a communication medium that became indispensable to regular life, governments merely extended copyright protection to the internet, thus creating ad-hoc and patched-up solutions to problems that were here to stay. In-depth knowledge of any subject is required to evolve an effective regulatory mechanism in relation thereto, and the internet is no exception to this rule. However, in an attempt to counter the recurring legal issues arising with regard to IP protection on the internet, the extension of copyright laws to the virtual world was seen as an immediate and workable solution. However, this 'solution' seems to have overstayed its welcome, as it is largely ineffective in doing what it was initially framed to do.

Bessen and Maskin have in fact opined that the best sort of intellectual property rights are strong enough to prevent direct copying and knock- off products, but are still weak enough to encourage the greatest amount of cross- licensing and sharing of information between competitors.[30] Orin Kerr proposes that the internet's ability to generate a virtual reality creates what he calls the problem of perspective in internet regulation.[31] According to him, many legal outcomes depend on facts, and the facts of the internet depend on which perspective we choose.[32] The term he uses to describe the virtual world from the user's point of view is the 'internal perspective' and that from the technician's point of view is the 'external perspective.'[33] For the user, the virtual world of

---

[29] *Supra* note 17.

[30] James Bessen & Eric Maskin, *Sequential Innovation, Patents and Imitation* (Dep't of Econ. – Mass. Inst. of Tech., Working Paper No. 11/99, 1999), *available at* http://www.researchoninnovation.org/patent.pdf.

[31] Orin Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003).

[32] *Id.*

[33] *Supra* note 31.

cyberspace is a legitimate construct. Hence, to the user, a computer connected to the internet provides a window to a virtual world that is roughly analogous to the physical world of real space. The external perspective adopts the viewpoint of an outsider concerned with the functioning of the network in the physical world rather than the perceptions of a user.[34] From this viewpoint, the internet is simply a network of computers located around the world and connected by wires and cables.[35]

Kerr highlights the problem of perspective using the example of the *MP3.com* case.[36] In this case, the court adopted the external perspective while ruling in favour of the record companies that sued the defendant company for unauthorized copying and distribution of music files across the internet to its registered users. Kerr opines that if the internal perspective had been adopted, the defendant may have been let off scot-free in this case.[37] Essentially, the problem of perspective arises depending on who uses the work, for what purpose and in what manner.

The approach of perspectives adopted by Kerr has been an inspiration for the authors to analyse the efficacy of a copyright protection regime for the internet. Applying this line of thought, the authors opine that there may be a problem of perspectives with regard to data put up on the net. This conflict crops up pertaining to the creator's and the end-user's points of view regarding the same piece of art or work. Hence, the creator's outlook may be understood from the moral and economic rights that she has over any work created by her - including the right to earn royalties from the work, the right of attribution, right to integrity of the work etc. The creator may be taking a risk of violation of these rights by putting her work up on the net, but she takes this risk on the assumption that there is an effective regime governing the internet that protects her rights.

On the other hand, the end-user is not too bothered with the rights attached to any work available on the net. The layperson assumes that anything available on the net for free is what it seems to be – free. This is nothing but the problem of perspectives. In Kerr's analysis as in the present one, the internet is a legitimate construct that allows the end-user to freely access data without any physical or other constraints. On the other hand, what the creator wants from publishing her work on the net may not be what the end-user perceives its use to be. Hence, the work may be put up on the

---

[34] *Supra* note 31.
[35] *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 849 (1997) (describing the internet as 'an international network of interconnected computers').
[36] UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000) (*Per* Rakoff, J.).
[37] *Supra* note 31.

net for a particular purpose by the creator but may be used by the end-user for another function not envisaged by the creator. The predicament is that the creator cannot recoup her expenses by imposing restrictions on access to her work, because of the large variety of alternative means available to the end-user today to access the work online. Consequently, the creator dissuades the end- user from trying to access her work freely. Clearly then, there is a constraint on the very purpose for which the internet is being used by the creator as well as the end-user.

The problem of perspective is relevant because the adoption of the correct regulatory mechanism depends on the perspective chosen.[38] This argument is expanded further in the section dealing with Creative Commons Licensing and the Tier Model.

III

POSSIBLE SOLUTIONS

It is clear that a tailor-made regime of regulation is required to govern something as dynamic as the internet, and that copyright is certainly not suited to this end. As one author said, without a legal monopoly, not enough information will be produced but with the legal monopoly, too little of the information will be used.[39] Hence, the authors propose two solutions to the governance of the internet, which modify the current regulatory regime to suit the nature of the internet.

Creative Commons Licensing

"Creative Commons aspires to cultivate a commons in which people can feel free to reuse not only ideas, but also words, images, and music without asking permission- because permission has already been granted to everyone."[40] Modern copyright law presumes that one size fits all. A Creative Commons (CC) license is a form of copyright license that can be linked to the World Wide Web. The purpose of CC licenses is to replace the default 'all rights reserved' approach with a more modest 'some rights reserved' approach that permits a variety of uses, subject to one or more limitations that the copyright owner has placed on the work.[41] A CC license bridges the gap between the concept of copyright that reserves all rights and the public domain where no copyright

---

[38] *Supra* note 36.

[39] ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 135 (1988), *quoted in*, Paul Goldstein, *Comments on a Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2573, 2574 (1994).

[40] Legal Concepts - CC Wiki, http://wiki.creativecommons.org/Legal_Concepts (last visited July 1, 2010).

[41] *See* Creative Commons, http://www.creativecommons.org (last visited July 1, 2010); *see also supra* note 10; *see also supra* note 17.

restrictions apply.[42] From the user's perspective, the presence of a CC license raises and answers the question, 'How can I use this?', as opposed to the question that is attributable to a copyright, 'Can I use this at all?'

Thus, the primary licensing terms that CC provides are:

- Attribution: rights to copy, distribute, display, perform and remix a copyrighted work as long as due credit is given.
- Non-Commercial: rights to copy, distribute, display, perform and remix a copyrighted work for non-commercial purposes only.
- Share Alike: rights to create remixes and derivative works under the identical license that the original work was published under.
- No Derivative Works: rights to copy, distribute, display and perform restricted to only verbatim copies of the original work.[43]

Creative Commons attempts to create a private solution to the problems of overprotection by building 'a layer of reasonable copyright' on top of existing law.[44] However it is important to note that while CC licenses create resources that are commonly accessible, these resources are not collectively owned. With a 'collective property', as opposed to intellectual property, the community as a whole determines how the resources are to be used. These determinations are made on the basis of the social interest existing in the property through mechanisms of collective decision-making. Creative Commons provides each rights-owner a chance to associate to a group that has a certain view of how copyright and property rights should be. It is easy to obtain the exclusivity of copyright, but sharing the work in a controlled way is a harder task.

Creative Commons has, together with an international community of volunteers,[45] created a set of open content copyright licenses and a web interface that enables rights owners to choose from a list of copyright licenses. First versions of the licenses were released in December 2002 and in nine years CC licenses have reached their third versions. After a licensor has chosen a license with the web interface, they can attach the selected license to the work as a hyperlink. After the license is

[42] Joshua But, *New Copyright Licences Allow More Sharing On Web ... Legally*, S. CHINA MORNING POST, Oct. 26, 2008.
[43] *Id.*
[44] LAWRENCE LESSIG, FREE CULTURE 264-65 (2004), *available at* http://www.free-culture.cc/freeculture.pdf.
[45] Creative Commons International, http://creativecommons.org/international (last visited July 1, 2010).

successfully attached, the website where the work is available will have a logo stating: 'CC licensed. Some rights reserved.'

In technical terms, CC is perhaps the first popular licensing project to answer the concerns of the European Copyright Directive which calls for rights holders to "identify better the work"[46] and "encourage the use of markings"[47] to "provide information about the terms and conditions of use of the work."[48] In particular, the set of CC licenses can be used to mark the copyright status of a work in order to enable users to quickly ascertain whether a desired use is permitted, and if so, on what conditions.[49]

A wide range of creators from around the world have already contributed to and drawn from this Commons. For example, CC licences have been localised and adapted to copyright laws in Hong Kong, making it the 50th jurisdiction in the world where they have become legally applicable. About 140 million objects around the world have so far been licensed under the system.[50] The surprisingly rapid growth of this system demonstrates the importance of marking information on the internet in a way that signals use relevance as well as topical relevance.[51]

CC is refreshingly innovative because it clearly accommodates the variable and vast nature of the internet as well as taking care of the problem of perspectives. CC in itself is a 'sequential innovation' over copyright law in the sense that it improves the working of copyright as applied to the internet. Copyright owners are denied a simple system to allow use of their work under the existing copyright regime. The permissions process can be cumbersome, if not prohibitive, and so, private actors have attempted to create and use modularized contracts so as to pre-authorize the use of their works.[52] CC simplifies this permits process by attaching pre-created licenses to the work, thus defining the scope within which the work can be used. Thus, not only is CC an improvement over copyright, but it also propagates sequential innovation by allowing 'next-in-line' creators to use original works to create new ones or even to facilitate improvement thereon.

---

[46] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (E.U. Copyright Directive), 2001 O.J. (L 167) 10.
[47] *Id.*
[48] *Supra* note 46.
[49] Aarthi S. Anand, *Readymade Licences as Obstacles to Blogging*, HINDU, Jan. 20, 2009; *see also supra* note 17.
[50] *Supra* note 42.
[51] *Supra* note 17.
[52] *Supra* note 10.

CC has been evolved to adjust the needs of the end-users with those of the creators, thereby addressing the problem of perspective. It takes into account the fact that different creators have different intentions with respect to the creative content of their work, and that this intention is not corrupted by unauthorized use of the creation by any end- user. Using the CC license, not only is the creator empowered to exercise the moral and economic rights that she wishes to own with respect to the work, but there is also a flexible, legally- accepted framework created within which any end- user can use the work. Since the law cannot be individually tailored to suit the needs of every creator, a CC approach fashions a flexible legal structure that gives enough freedom to every creator to allow what she wishes others to do with the work, without having to tolerate its use in any manner not desired by her.

The Tier Model: A Business Solution

Another feasible solution that the authors propose for enhanced internet regulation within the scope of the issues raised by this paper is the Tier Model. Inspired roughly from Yochai Benkler's Theory of Layers,[53] this model proposes that no regime of regulation whatsoever should be imposed directly on the internet, and consequently, on its users. Instead, the law should seek to regulate the internet by regulating the models used to conduct business over the internet. This makes the need for a copyright regime redundant, focusing instead on the very nature of the internet as a medium of interconnectivity, accessibility and advertising.

The ad-based model, deployed by internet giants like Google to earn revenue, can be used to depict how the Tier Model may work. The Tier Model is based on the premise that the internet is a free market wherein every player aims to earn the maximum profits possible. It is assumed that websites on the internet are put up for a particular purpose, which has a profit or other personal motive behind it. Hence, persons advertise the works of a particular creator and host that work in order to increase the number of visitors to that website – also called 'eyeballs.'[54] An increase in the number of eyeballs increases the chances of visitors to the site using the services provided by the website and augments revenues.

---

[53] Professor Yochai Benkler's Theory of Layers provides an effective approach to a multi-level analysis of access regulation. Professor Benkler's theory addresses not only the content layer of digital communication, but also the code layer and the actual physical infrastructure. YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006).

[54] *Supra* note 12.

The Tier Model proposes that what should be controlled is not the content posted, but the way or the means through which the content or work of the creator is posted, and the way in which it is advertised. In effect, the Tier Model proposes that the content of advertisements that declare the existence of that particular work on that website is to be regulated. By doing so, i.e., by telling the intermediary[55] that she can't advertise the content of the work in a way that violates the creator's permit to use the work (on the assumption that the work is CC licensed), the law protects the creator's rights, and warns the end-user of the limits to which the work can be used. This, of course, is just one example of how business models can be regulated in order to protect data over the internet.

Another example of the application of this model is the way Jstor works. Jstor is an online digital library that caches a number of journals on subjects of philosophical and sociological interest. It is subscription-based and allows users to access content originally published in journals which hold the copyright. Consequently, what is regulated is the way users are allowed to access the content and not the content itself. So, instead of letting users download for free, Jstor only allows the user to purchase and then download the content online.[56] This reduces the risk of users interfering with the content and also allows them to access content, albeit in a limited manner. In this example, the Tier Model is used to restrict the manner in which the websites allow access to content. This is a way to indirectly restrict access without touching the copyright on the content.

If there exists a law or bye-law that restricts proprietors of websites and service providers from providing or displaying content in a particular manner, say by restricting downloads as in the case of Jstor, what the law is doing in effect is regulating the model on which the operation of the site depends, instead of creating an IP over the content itself. This in turn clears the haze surrounding the problem of perspective, as in this case, the only perspective being applied is that of the proprietor. Any kind of use of the creator's material by the proprietor that is illegal or not in conformity with the law will result in liability. However, in this case, the internet is still a legitimate construct where knowledge and content is free. The qualification remains that such access is not unlimited but restricted by virtue of the kind of services provided by the proprietor of the website. Hence, the user may continue to legally access and use the content but only in one possible manner – the restricted way, as defined under the law. Such a law would be workable

[55] The service provider who posts or allows the author to post his creation on the net.

[56] *See* JSTOR: The Archives, http://www.jstor.org/page/info/about/archives/index.jsp (last visited July 1, 2010); *see also* Frequently Asked Questions, http://www.jstor.org/page/info/help/faq.jsp (last visited July 1, 2010).

because in this case, access to the content, and consequently its authorized use, depends solely on the medium in which content is published. Other factors like the nature of the content, i.e., whether it is a literary or artistic or cinematographic work, or the question of whether the content *per se* is protected, do not come into play. Hence, this law would be medium-specific, wherein what is regulated is the medium of publication of the content, rather than the content itself.

The other perspective we are concerned with is that of the creator. Clearly, the problem of copyright violations occurs because the user's perspective doesn't match that of the creator. CC licensing may solve this problem in part by making the creator's perspective clear to the user by virtue of the nature of license attached to the work. The Tier Model may be useful in removing the problem of perspectives because it adopts a perception of the internet which is neutral. The perspective adopted is that of the proprietor, the person who facilitates the interaction between the user and the creator through the internet medium.[57] The role of the proprietor of the site in the virtual world is similar to the role of the publisher of a book in the real world. The proprietor of the website has an economic interest in putting the creator's content up on his site.[58] This incentive may be in form of the number of the eyeballs he receives, the number of downloads from his site, etc. Hence, the rationale behind adopting the proprietor's perspective is that he has the best interests of the creator as well as the user in mind – the former, because he becomes responsible to the creator for ensuring that the material is not abused because it is put up on the internet, the latter because he must still try and make the work as widely accessible as possible.

It is also clear that this model works best when the work is CC licensed, i.e., the creator has previously permitted the work to be used in an ascertained manner. Usually, no creator who wishes to propagate her work will prevent advertising to her own detriment. But using this model, she can also impose restrictions on the way the advertisement depicts the work to the end-user. In addition, this model acts as a good check against the defense usually taken by intermediaries that they were unaware of the infringement taking place. This was a concern that came up with the suit filed against Napster by major record labels in the US, when the file-sharing giant was shut down on grounds of copyright violation. Yet, this suit encouraged a 'tsunami' of open P-2-P file sharing

[57] On the emergence of new intermediaries in the digital world, *see* Michael W. Carroll, *Creative Commons and the New Intermediaries*, 4 MICH. ST. L. REV. 45 (2006).

[58] For the functions intermediaries play in the commercial dissemination and exploitation of creative works, *see supra* note 2.

that was unencumbered by DRMs.[59] This development led many record labels to sue individual end-users who were found to have downloaded music from the internet illegally.[60]

IV

CONCLUSION

Knowledge is a public good in that it cannot and should not be the personal domain of any one creator. The internet is an ideal forum for the dissemination of knowledge due to its all-pervasiveness. Alternative internet governance mechanisms should be explored that can fulfill this objective and still serve as viable regulatory models. Any solution proposed should ensure that knowledge dissemination is not restricted while also considering IP infringement as a real threat to creativity – the solution should bridge these two considerations.

It is quite evident that internet governance is not a simple matter. The internet, in particular, is a highly interactive environment with sequential innovation. Attempts to impose additional intellectual property protection or to expand existing protection might be detrimental because they fail to consider the value of creative imitation.

The internet has created new problems for copyright owners, who see their works distributed and copied throughout this immeasurable network. Piracy and copying of protected works have always existed, but never on the scale that the internet so simply facilitates. Many solutions have been offered, but to regulate any distinctive institution, activity or phenomenon, the law needs to take into account the nature of the subject, its complexities, its weaknesses, possible loopholes, etc. Therefore, in the absence of the aforementioned considerations, copyright law, on its own, is evidently unsuitable for governing a dynamic forum like the internet, primarily due to its inflexibility and redundant assumptions.

However, it should be remembered that in the absence of an elaborate, full-fledged legal and regulatory regime to protect content over the internet, copyright cannot be abolished. For instance, even the solution proposed in this paper, i.e., CC licensing, is based on copyright. Although Lessig argues that these licenses are 'bullet-proof',[61] to date, they have not been tested even in the U.S.

[59] *Supra* note 12.
[60] *Supra* note 12.
[61] *Supra* note 44.

courts, and Creative Commons itself gives no such guarantees.[62] As long as enforceability is unclear, some prohibitive uncertainty remains.[63]

To illustrate this point further, Goss provides an example to illustrate the existing ambiguities in relation to CC licensing where an educational website displays an article but requires a membership password to access it. Would this amount to commercial use? Moreover, if the same website uses advertisements to support its publishing costs albeit without a membership system, then is that 'primarily intended for' or 'directed towards' commercial use? It is thus evident that without clear interpretations of its licensing terms, CC licensing still has a long way to go in proving itself as a pragmatic replacement to copyright.

Moreover, it has further been debated as to whether, instead of extending the public domain, CC licenses have introduced prior permission for work which may have no commercial value.[64] On the premise that CC is the most commonly used 'prêt-a-porter' (or readymade) and easily embeddable licence regime, Aarthi Anand argues that many blogs and other non-commercial forums would not be copyrighted if creators had to pay for the cost of drafting a legal notice. In other words, in the absence of CC licensing, creators would have been willing to incur legal expenses only for work they intended to commercially exploit, with all non-commercial work remaining free from copyright. Thus, the real test of CC licensing's contribution to the public domain should not be the popularity of the CC licence but a future creator's ability to draw on commercial work hitherto prevented by copyright.[65]

Accordingly, the above solutions proposed by the authors can be used as viable complementary mechanisms to the existing legal regime as the said solutions merely control the dissemination of works, and do not protect works as such. Hence, these solutions may be effective in stopping or reducing unauthorised access of protected works on the internet.

---

[62] *Supra* note 10.
[63] *Supra* note 10.
[64] *Supra* note 49.
[65] *Supra* note 49.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 6, 2010

BOOK REVIEW: CYBER LAWS, JUSTICE YATINDRA SINGH (UNIVERSAL LAW PUBLISHING CO., 2010)

Prof. Ashwani Kumar Bansal[*]

The phenomenon of the internet has revolutionized the world – the way we communicate, do business, store information, run machines or even open river gates to control the production of electricity and maintain water levels in reservoirs. All of this happens at the mere click of a mouse while sitting at distant places through signals sent via satellites and novel devices based on digital technologies. The internet is largely a network of computers spread all across the world and connected to one another through hardware, routers and cables. There are numerous private or government agencies that keep our precious data in electronic form. Anyone who has a bank account is being served by networked or stand-alone computers. We use ATMs, debit cards and credit cards for shopping and use email, cell phones and SMS for communication. Thus, in the present digitized world, no one can really claim to be unaffected by cyber law altogether.

Cyber crimes such as online banking frauds, source code thefts, virus attacks, phishing attacks, email and website hacking, etc. have become common place. It is for these reasons that 'cyber law', that is, the legal aspects of the cyber world has become important. The cyber law of India is mostly found in the Information Technology Act of 2000.[1] Necessarily, all the good about technology can always be used in an adverse manner, and therefore, the role of the law is to maximize the good and minimize the adverse.

The book 'Cyber Laws', by Justice Yatindra Singh, a sitting judge of Allahabad High Court, has been published by Universal Law Publishing Co. and is now in its fourth edition. The book is a comprehensive guide to the various legal issues which have arisen as a result of the unprecedented growth of the internet. It covers both academic and practical information regarding technology-related issues and the underlying legal principles which have been applied in these areas. Part I of the book has 146 pages of commentary and Part II contains relevant Acts, rules, notifications,

[*] Professor In-charge, Law Centre-I, Faculty of Law, University of Delhi.
[1] Information Technology Act, 2000, No. 21 of 2000 (hereinafter 'IT Act').

circulars, etc. in 276 pages. The book provides an overview of the cyber law scenario in India. The material is well researched and clearly described in thirteen concise chapters.

Justice Singh has included multi-faceted introductory material that also covers new developments in other jurisdictions. He simplistically guides the reader and provides suitable inputs at all times. He does not cling to a rigid structure and attempts to incorporate diverse information in the book on all relevant occasions. He has included pertinent case law and discussed the implications of the same for future legal developments. The author uses foreign case law to explain propositions in relation to the law in India. He explains the *Pettigrew* case[2] and the *Myers* case[3] so as to inform the reader about the acceptable level of amendment that can be brought about in the law of evidence in India through the IT Act.

The book not only explains the law as it is but also informs the reader about the practical aspects of using information technology. It is necessary for a reader to comprehend why Justice Singh is explaining things that appear un-connected at first glance. However, I am quite confident that at a subsequent time the reader will find out how these nuggets that amount to no more than two or four pages have helped clarify issues. It is this attention to detail that he has given that one may not find in other books on cyber law. The underlying logic appears to be that once a person knows something, only then he realizes how much he does not know and may crave for that knowledge. I must therefore congratulate Justice Singh for accomplishing this onerous task.

Justice Singh takes the reader to the UNCITRAL Model Law on E-commerce, the basis for the IT Bill of 1999 that resulted in the IT Act. The IT Act provides legal infrastructure for e-commerce transactions, recognises electronic documents as legal evidence, opens up business opportunities for digital certificate companies, paves the way for e-governance transactions, and creates specific provisions against cyber crimes. In 2002 itself, it was felt that the IT Act needed amendments to address current issues and challenges in the cyber world. The Inter-Ministerial Working Group on Cyber Law and Cyber Forensics was established in November 2002 in order to pursue this object. The present reviewer was appointed as the Member-Secretary of this group and on the basis of the deliberations in this group and other related groups, an expert committee was later constituted to suggest amendments to the IT Act. The amendments suggested were introduced in Parliament as the IT (Amendment) Bill of 2006 which was modified and passed by Parliament on 23 December,

[2] R v. Pettigrew, (1980) 71 Crim. App. 39 (C.A.) (U.K.).
[3] Myers v. DPP, [1965] A.C. 1001 (C.A.) (U.K.).

2008. IT (Amendment) Act of 2008 received the assent of the President of India in February 2009 and then was brought into force on 27 October, 2009. The book covers all the important changes introduced by the IT (Amendment Act) of 2008. The book also incorporates several important provisions of the Communication Convergence Bill of 2001.

The book is divided into two Parts. Part I deals with different aspects of cyber laws with discussions on various topics, controversies and possible solutions. The book discusses several foreign statutes and provides citations using online sources in order to enable easier access. Chapter I deals with the historical background of the IT Act and in 10 sections refers to the different provisions of the IT Act. It also includes a brief section on Electronic Funds Transfer. Chapter II introduces the basic concepts of Intellectual Property Rights and also discusses issues in relation to international organisations and important treaties. In Chapters III and IV, the author discusses computer software and copyright in an interesting fashion and introduces the idea of 'Copyleft.' He analyses the existing controversies in relation to computer software and patents and includes a concise discussion on the idea of 'Invention.' He also introduces the reader to the new field of business method patents. Chapter V discusses the system of protection in relation to trade secrets and reverse engineering and talks about the important issue of disassembling copyrighted software. Chapter VI may be an eye opener to those who have not come across the terms 'open source code' and 'proprietary code' and the myriad issues relating to the open document format. Chapter VII deals with font licenses and Justice Singh suggests that the Government of India should release fonts on a copyleft basis and grant the permission to use and modify the same through an open source code. Chapter VIII deals with IPR in cyber space and the legal problems faced by websites hosting illegal content and internet service providers. Chapter IX deals with the protection of semiconductor topography as per the Semiconductor Integrated Circuit Layout-Design Act of 2000 and details the different advantages and disadvantages of the protection afforded under the Act. Chapter X deals with e-commerce and taxation in a nutshell. Chapter XI discusses the grey areas of privacy and 'cyberslackers.' Chapter XII deals with how information technology can help in case management, court management and self improvement and bring about major changes in the legal system. The conclusion of the entire discussion is stated in brief at the end.

Part II provides useful and important legal instruments including Acts, rules, regulations, treaties, notifications, policies, guidelines, etc. These instruments are updated and so provide an invaluable resource for further research.

In sum, the book aptly discusses how some persons have been misusing the phenomenon of the internet to proliferate criminal activities in cyber space, how such activities can be curbed through suitable law, and how a pressing challenge faces the cyber law regime in India. The book provides concrete suggestions regarding the manner in which the flaws, loopholes and ambiguities observed in certain provisions of cyber law can be tackled and encourages the reader to engage with the length and breadth of the entire subject.