Chapter 7

CONCLUSION

Internet technology highlights many ambiguities with respect to human rights and available legal protections and the difficulties of their enforcement due to technological inadequacies and human frailties. The future of digital rights management, for instance, depends on choices with respect to the evolution of the copyright law and its interpretation. Jon Bing[1043] emphasizes the interdependence of the evolution of digital technologies, the law as a means of regulation and control, and the potential for inconsistencies between the interpretation of the law and its implementation in computerized code. Once regulations and rules are automated, they are extremely difficult to subject to judicial review. Following Lawrence Lessig's[1044] argument that the code of cyberspace becomes the regulator and this might create situation of 'technology [is] implementing the law'. Increasing diversity in the bundles of rights offered to users of protected information is likely and differences in the negotiating power of right holders and users may lead to a need for new forms of consumer protection. Software agents might become negotiators of legal positions and be guided by formalisms in the software code that may not be consistent with the real world position.

Cyberspace regulation continues to mean different things to different people. For many stake holders, particularly in the libertarian atmosphere of the online world, the mere mention of the word regulation is enough to generate extremely negative reactions. For others, cyberspace regulation generates images of a return to a simpler and more circumscribed lifestyle, when human action seemed much more predictable and when people could more easily rely on certain time tested principles to guide their daily affairs. Those holding such a view do not threatened by

[1043] Bing John, Code Access and Control, Human Rights in the Digital Age, (Ed by Mathias Klang & Andrew Murray) The GlassHouse Press, London, 2005 at p 203-211
[1044] Lessig, Lawrence, Code and other laws of Cyberspace, Basic Books, New York, 1999

government action in cyberspace, rather by lawbreakers and anarchists who might use this new communications medium to further their own nefarious ends. On some level, particularly for certain problem areas as far as human rights are concerned; the internet itself is seen as the enemy here. Regulation is viewed as a panacea, and the government is perceived as not doing enough. But regulation will solve all the problems of cyberspace entities is a distant dream. Yet these opposing positions are constantly being eroded by emerging events and changing realties. Those who maintain libertarian positions may be confronted by a new problem that leads them to argue for some sort of regulatory solution. And those who have been lobbying for additional, restrictive law may find themselves in the surprising position of responding to a new issue by arguing that things should simply be left alone.

Architectural considerations, as we have seen in Chapter 1, further complicate this picture. No matter what view of cyberspace one adopts, it must be recognized that on some level this is not a physical reality, but an audio visual representation created and made possible by software code. Any discussion of regulation issues in this area can therefore lead quickly to central questions regarding appropriate analogies. For example, it has been argued that every communication taking place in a networked environment should be viewed as analogous to a phone conversation, and that both e-mail and World Wide Web are nothing more than graphic representation of the conversation created through the magic of software code. According to this view, the regulation question is very simple. All the rules we need are those that have already been worked out for telephones.

But this view is typically countered by noting that digital technology has enabled online users to accomplish many things in a networked environment that were simply not possible on a traditional phone, such as taking virtual tours of museums, viewing live scenes from distant locations and creating digital copies of other people's work. In addition, on some level, an online presence can quickly become very much akin to an offline presence. Establishing interactive business in cyberspace, for example, is in many ways no different than opening a new commercial enterprise in the building down the street. Which rules should apply?

Those for telemarketing or those for brick-and-mortar operations ? And how should the unique, code based aspects of online communication be factored in? Should speed, scale and a greater level of anonymity make any difference in the end? Or can it be expected at some point new software code will adjust for speed, scale and anonymity?

In the light of these complications and inconsistencies, many people are beginning to gravitate away from all-or-nothing positions regarding regulation. Yet the continued rhetoric accompanying these debates has led to the persistence of certain overarching generalizations regarding the current state of affairs. In the aftermath of the Feb 2000 denial-of service attacks[1045] against major commercial websites, for example, the media was filled with comments purporting to explain the parameters of governmental control. Major newspapers declared that the Internet is neither owned nor regulated by the government. Security experts described the online world as "an open system without set standards of regulation". Former President of America Clinton, in a Cyber Security Summit observed that 'one of the reasons the Internet has worked so well is that it has been free of government regulation'.

The fact that promotion and protection of human rights is the primary responsibility of the States in the physical world an they do so in the interest of society but governments will be interested in promoting human rights in cyberspace only when they can have certain control over the activities of the cyberspace entities. This is where the actual problem lies in protecting and promoting human rights in cyberspace.

Human rights are universal, inviolable and inherent in every human being. These rights have to be promoted and protected both in the virtual world like cyberspace and physical world. Internet technologies empower every user to express his views

[1045]See CNN.com, Cyber attacks batter web Heavyweights, available at http://archives.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html , visited on 24 Nov 2004; Denial of Service (DoS) attacks are attacks on compputer networks , which cause networked computers to disconnect from the network or just outright crash. For example, a teenager using very simple DoS tools managed to cripple the web sites of large companies like Yahoo and Amazon during a series of attacks in February 2000. These attacks are sometimes also called "nukes", "hacking", or "cyber-attacks".

and opinions freely in an inexpensive way. The most democratic right of all, freedom of speech and expression, now offers a way to participate in democratic process for all of us. Right to privacy, most valued right by civilized men, if not properly protected faces the danger of being abused by other entities of the cyberspace. For an economic human right like copyright, the internet offers both opportunities and threats to the owners of creative works. If these basic human rights are not enforced, then their exercise in cyberspace becomes meaningless. And this is where the jurisdictional problems created by internet technologies have to be appropriately resolved.

It is quite obvious that there is a potential clash between laws protecting human rights and the principle on which the Internet works i.e. unrestricted flow of information across national boundaries. The most important human rights affected by internet communication include free speech, privacy, right to reputation and economic rights like copyright.

An absolute right to free speech means that those whose privacy and reputation is infringed by that speech have no remedy. An absolute right to privacy restricts free speech of others. Even within a single jurisdiction, the law must balance two rights by placing restrictions on each. Internet being a global media, the balancing of these human rights assumes greater significance and becomes global in nature.

Once information crosses national borders, as is almost inevitable with internet communications, additional conflicts arise. Because the rights of privacy and free speech are not absolute most states impose limitations on them, either for the protection of other citizens or to preserve elements of the national and economic interest[1046]. These limitations widely vary from State to State, as legislators and

[1046] For examples, European Convention for Protection of Human Rights and Fundamental Freedoms, 1950, Art.8 (right to respect for private life): '2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being for the protection of the rights and freedoms of others'; and Art.10 (freedom of expression) :'2. The exercise of these freedoms, since it carries with it duties and responsibilities , may be subject to such formalities , conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interest of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the

courts take differing views of the necessary balance to be struck. Because, say, a webpage is accessible from all jurisdictions, an author will only be able to comply with the differing national limitations by complying with the most stringent limitations on his freedom of speech and similarly may need to observe the highest privacy standards.

In practice those limitations which protect individual interests by giving the affected person a right of action will rarely have substantially restrictive effects. The normal remedy is one of damages and cross-border litigation is likely only for the most serious infringements. More serious are the limitations which be enforced by national authorities , whose actions will in many cases have an extraterritorial effect as we have seen in LICRA V Yahoo Inc., decided by French court and Dow Jones V Gutnick, decided by an Australian court.

Freedom of speech and expression is the most admired right in cyberspace. The internet has provided a great platform for exercising this basic human right in an unprecedented way. Through blogs and websites almost every net user has become author. Technological change presents new possibilities for freedom of expression, shows the value of free speech in a different light, and makes particular features of freedom of speech particularly salient. These features include interactivity, mass participation, nonexclusive appropriation, and creative transformation. This in turn leads us to a new conception of the purposes of freedom of speech, which we can call the promotion of a democratic culture. However, these same technological changes also create new forms of social conflict, as business interests try to protect new forms of capital investment. This leads, in turn, to attempts to protect and expand rights in intellectual property and in the control of telecommunications networks. These rights claims clash with freedom of speech values in ever new ways; and the attempt to protect property rights in capital investment leads to competing visions of what freedom of speech is and what it is not.

---

reputation or rights of others, for preventing the disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary'.

Finally, as technological innovation alters the social conditions of speech, the technological and legal infrastructure that supports the system of free expression becomes fore grounded. As a result, free speech values must be articulated and protected in new ways, in particular, through the design of technology and through legislative and administrative regulation of technology, in addition to the traditional focus on judicial doctrines that protect constitutional rights.

As the world changes around us, as the possibilities and problems of new technologies are revealed, our conception of the free speech principle begins to change with them. Our sense of what freedom of speech is, why we value it, and how best to preserve that which we value, reframes itself in the changing milieu. And as we respond to these changes, retracing our steps and rethinking our goals, we eventually come to understand what the free speech principle is about, and more importantly, what it always was about but only now can be adequately expressed. That experience is not the experience of making something new. It is the experience of finding something old, of recognizing principles and commitments already dimly understood which suddenly are thrown into sharper focus by the alteration in our circumstances and living styles.

Free speech should be free in cyberspace. American courts have been leading the world when it comes to free speech issues. But the standard of scrutiny varies from country to country. Applying American standards of free speech scrutiny may be difficult for other countries, especially when religious matters are involved. So the ideal way may be to apply the standards used in defendant community. In this regard individuals and other entities must have consensus that there is no absolute right and free speech is no exception. The best way of regulation seems to be self-regulation. Many chat room activities and blogging activities are being regulated by the groups themselves. Whenever an offending statement appears, the maker is being warned and sometimes removed from the group. But here again there may arguments of bias. There are no standards to measure and declare whether a particular statement made by the netizen is offensive or not?. This is subjective and not quite easily resolved. As far as

indecent or obscene material is concerned, Miller test formulated by US Supreme Court merits high as the test prescribes contemporary standard as a test for indecency or obscenity. More interestingly US District court has taken the view that Free speech right is available only against government and not private persons[1047]. This may cause lot of concern for free speech activists in cyberspace as most of the actors in cyberspace are private persons. Government of China is ordering to censor the content to private companies like Google and Yahoo. This kind of regulations poses difficult problems for the netizens free speech right. Right to speak anonymously must be regarded as part of free speech right .And free speech should not be allowed to be abused in cyberspace. Right to reputation of persons must be suitably protected and threatening and hate speech must be prevented. These things are possible only if certain restrictions on are imposed on free speech. The balancing of free speech with other fundamental rights is delicate and maintaining harmony is difficult, but policy makers must make an effort to achieve the right balance among these human rights.

Privacy being a basic human right, we must recognize that a vision protective of information privacy in cyberspace will be singularly hard to maintain. Cyberspace's essence is the processing of information in ways and at speeds unimaginable just years ago. To retard this information processing juggernaut in the name of privacy seems anti-technology, even anti-progress. It cuts against the hackneyed cyber-proclamation that information wants to be free. Nevertheless, this intentional application of friction to personal information flows is warranted. If profit seeking organizations are instituting such friction in the name of intellectual property, individuals should not be chastised for doing the same in the name of privacy. Historically, privacy issues have been an afterthought. Technology propels us forward, and we react to the social consequences only after the fact. But the amount of privacy we retain is to use a decidedly low-tech metaphor a one-way ratchet. Once we ratchet privacy down, it will be extraordinarily difficult to get it back.

[1047] America Online Inc., V Cyber Promotions Inc., United States District Court, E.D., Pennsylvania, 1996, 948 F.Supp.436

More disturbingly, after a while, we might not mind so much. It may dawn on us too late that privacy should have been saved along the way.

Protection of privacy interests of netizens is actually is in their hands. If netizens refuse to disclose their personal data, marketers have to employ technical measures which can be legally prevented. But netizens in US and other developing countries are willingly participating in personal data commodification. We need to have international treaties to share the personal data of netizens of various countries. The safe harbor treaty between US and EU is one such example. The way US looks at personal data, as contractual obligations, is highly inadequate for cyberspace transactions. EU model of treating informational privacy as human rights quite suitable for cyberspace transactions.

Both intellectual property rights and human rights deal with the same fundamental equilibrium. On the one hand there is a need to define the scope of the private exclusive right that is given to authors an incentive to create and as recognition of their creative contribution to society broadly enough to enable it to play its incentive and recognition function in an appropriate and effective way, whilst on the other hand there is the broader access to the fruits of author's efforts. Both intellectual property law and human rights try to get the private public rights balance and as such there is no conflict. Both areas of law however not define that balance in exactly the same way in all cases. There is therefore compatibility between them, rather than a consensus. In cyberspace most rampantly violated right is this human right, copyright.

The growth of Internet, especially the WWW has created a new cyberspace for copyrights exploitation. The analysis of copyrights in cyberspace reveals a mixed result of new opportunities and threats. Cyber technology had offered new ways of commercialization or exploitation of copyrights by business firms and individuals.

These new ways have enabled greater scope for global expansion and market reach around the world, promising huge potential for generation of revenue or other means of returns. However, these new opportunities pose parallel threats many of which even undermine the very rights of the copyright holders. The magnitude of threats is unprecedented with the technological feasibility making it possible not only for easier piracy but also for easier distribution of such pirated works to masses by a click of a button. Such threats often outweigh the opportunities offered by the cyberspace, and this calls for increasing regulation of cyberspace to protect copyrights. The present cyber anarchy has created a range of legal challenges to regulators. The ubiquitous nature of Internet has made many of these challenges international in nature, calling in international copyright regimes for greater regulation of cyberspace. The cyberspace, as such is unregulated and various transactions carried out in the Internet surpass the national regulatory controls. The technological feasibility to surpass national governments or regulation causes doubts as to the effectiveness of any single domestic regime or a select group of domestic regimes to regulate the cyberspace. Moreover, many of the domestic copyright regimes are relatively new ones and as such may be ill-equipped to address copyright in cyberspace. This calls for increased international co-operation for the regulation of cyberspace including the protection of copyrights.

Many of the new forms of transactions in cyberspace are highly technology oriented and any legal efforts to regulate the same have to go hand in hand with the technological growth. Law and technology, needs to be combined for effective solutions for many of the cyberspace challenges including those related to copyrights. In the context of copyrights many legal principles need to be developed or settled to determine the legality of the transaction in question. Many such pertinent questions related to copyrights in cyberspace have to be clearly settled at an international level. Lack of internationally agreed principles relating to copyrights in cyberspace gives room for divergent domestic standards. The continued evolution of cyberspace and the rapid growth of cyber technology create a state of flux, prompting a delay in legal response. There are also debates as to the

potential of existing international regimes versus the need to create new regimes to address copyrights in cyberspace. Also mindful are the need to balance the conservation of online technological advantages versus the urge to regulate copyrights in cyberspace. The urge to develop regulatory regimes of copyrights in cyberspace is also hindered by the digital divide existing between the developed and the developing world. The entire complex set of cyber copyright issues indicates a range of potential challenges in developing international principles to protect copyrights in cyberspace.

It is quite difficult to apply traditional intellectual property law in cyberspace. And it is more difficult in case of copyright protection. Though technology empowers copyright holders to protect their works it defeats the fair use purposes. Right of the authors to regulate the access and use to their work through digital rights management is quite unacceptable. However, norms that would balance the interests of the user and author are highly desirable. Even then requirement of international institute to protect and enforce copyright enforcement have become inevitable.

The most significant recurring theme is the challenge to our concept of jurisdiction. Legal systems have created an enormous body of doctrine governing the relationship between the territory of the nation state and the legal right to exercise jurisdiction. Although the Internet has not rendered the concept of nation state redundant, the fact that actions in ether[1048], of an unknown person in an unknown location, can bring about the most tangible of consequences renders the connections between territory and jurisdiction less relevant than in the past. The difficulty lies not only in the fact that no solution has yet been found to the problem, but also in that no solution has even appeared on the conceptual horizon.

Does the issue of jurisdiction hold more relevance for legal theory than practice? Legal theorists delight in musing over conundrums and technicalities. Often in

[1048] The air, when it is thought of as the place in which radio or electronic communication takes place.

practice, however, these intellectual puzzles rarely influence practical reality. Recent examples of international cooperation in law enforcement might demonstrate that, in some cases, the problems of jurisdiction are surmountable when need be. However, for every high-profile case such as the Mellisa Virus[1049], there are innumerable cases of illegal or improper conduct that might affect the proper exercise of human rights in cyberspace, simply cannot, as yet, be regulated. Whether and how the global society solves the problems of jurisdiction will be a key element in the development of the true Internet jurisdiction.

The topic of jurisdiction leads directly to the drive for the harmonization and globalization of laws. All too often broad aspirations for harmonized laws are expressed in the hope that this might be the panacea for the Internet age. When examining this issue in the future, we should be aware that the espousing rhetoric of harmonization in much more convenient than actually producing it. There are certainly benefits to be gained from international cooperation indeed; to avoid such developments would be to take the stance of Ostrich. Many normative developments applicable to the internet begin their journey to national implementation in the realm of international negotiations and policy discussion. Nevertheless, expressions of international cooperation and aspirational international instruments should be regarded with a healthy skepticism.

In turn, the driver for harmonization highlights the increasing importance of international organizations, including the United Nations, the European Union, Organization for Economic Cooperation and Development, and the World Trade Organization, to name but a few. Each society's normative frameworks provide the benchmark for regulatory stance. The vector sum of various lobby groups produces the final outcome. As the subject of normative debate increasingly international, so too do lobby groups. International organizations are frequently co-opted to represent the interests of large international players. These players might be governmental,

[1049] A computer virus which was propagated through macros of Microsoft word 97 and 2000 documents. If launched this macro virus will attempt to start Microsoft outlook to send copies of the infected document via e-mail up to 50 people in outlook's address book as an attachment. See for details http://www.melissavirus.com/

corporate or otherwise. For example, it is clear that the United States policy on encryption has influenced both the polices of other nation sates and those of international organizations.

Experience thus far addressing the challenges posed by the internet community in the European Union (EU) and United States (U.S.) suggests that existing law can sometimes be applied with relative ease to Internet activities and that existing law can sometimes be adapted to reach Internet activities. However, in some instances, new laws seem to be needed. When old laws do not fit and cannot easily be adapted, it may be necessary to go back to first principles and consider how to accomplish societal objectives in the new context of the Internet. Decisions about the law of Internet, whether carried out by judges, legislatures, or regulators, will have an important impact on the kind of information economy that will emerge. The EU is to be commended for realizing that regulating the Internet is about more than information infrastructure and economics. Deciding how to regulate the Internet is also about constructing an information society in which social and cultural values can be preserved.

7.1 Recommendations

Thus, in the light of the analysis set forth in this research work, we conclude and recommend by reviewing certain basic principles that can inform any future oriented approach to cyberspace regulation for the promotion and protection of human rights;

(1) When addressing human right issues, entire range of regulatory approaches have to be considered including litigation, legislation, policy changes, administrative agency activity, international cooperation, architectural changes, private ordering and self-regulation. In cyberspace, it is reasonable to assume that a creative combination of approaches will be more effective than any single regulatory strategy.

(2) In order to ensure that the Internet retains its ability to serve as a dramatic and unique marketplace of ideas, it is essential that regulatory frame work

must continue to respect the autonomy of individuals and groups in the online world. Internet started as a free medium of communication and its true nature must be maintained. This guarantees the fair exercise of basic human rights in cyberspace.

(3) The status quo, however, should not necessarily be viewed as inviolable. Certain aspects of the online world can and should be changed. And solutions can be crafted for individuals to exercise their rights which will not impact on other cyberspace entities. For example, exercise of individual netizens rights should not affect the rights of the commercial organizations to their detriments. For example commercial organizations right to send unsolicited mails to market their products should not harmed by over-protecting the rights of individuals. We need to be careful about all-or-nothing arguments that view any change in the law for particular situation as the first step down a slippery slope. Restricting the rights of cyberspace entities does no mean that there would be prohibition on the rights of these entities.

(4) Care must be taken to avoid viewing cyberspace regulation issues in a vacuum and the classification of problematic activity into one of four categories is an important first step in this process. By determining whether certain online behaviour constitutes dangerous conduct, fraudulent conduct, unlawful anarchic conduct or inappropriate conduct, patterns can be identified and helpful signposts can be pinpointed within a larger context. In addition, such an approach recognizes that Internet related problems can be as varied as the range of issues that must be addressed by legislators and policymakers in the offline world.

(5) If we are committed to maintaining the present day version of the Internet, then consensus among the various stakeholders will be an essential component of any effective problem solving approach. Under current conditions, given the highly participatory nature of the online activity and the distributed, anarchic design of cyberspace itself, there are hosts of ways to get around most restrictions that may be imposed. In addition, new

architectural changes can often be countered by other code based solutions. Thus a proposed regulatory approach may not be possible unless those that have the ability to resist agree to go along with the plan. And the list of such persons and entities would include not just the government regulators , but also Internet advocacy groups, virtual communities and individual netizens. In this regard it is pertinent to note the role played by organizations like ACLU[1050] and EFF[1051] , in protecting the free speech in cyberspace when they challenged the provisions of Communications Decency Act.

(6) Any decision regarding how to regulate human rights must necessarily begin with the clear understanding of the nature of this new medium, Internet and the challenges and opportunities raised by it. Certain conduct may be no different in cyberspace than it is in the offline world, while other conduct may be so dependent on speed, scale and anonymity that it may require a very new regulatory approach.

(7) The inherent limits of our legal system must always be addressed and taken into account to address the problems of the online world. Human Rights prevail universally only if the rule of law prevails universally. Introduction of computer viruses to the internet is possible from any country. As we have found in the case of 'I Love You', (where Philippines has law punish the offender), a country may be lacking laws regulate unlawful activities in cyberspace. However, both the existing rules and any prospective new strategies that might be developed under the traditional national law model should invariably considered first. Statutes, case decisions and administrative agency activity have already made a difference in certain key areas in US. And while no enforcement operation is ever completely successful, a rule that modifies the behaviour of most people can indeed constitute a reasonable solution in the end.

(8) From the global perspective, it is important to have an international institute which works with the national agencies. National laws may have value in

[1050] www.aclu.org
[1051] www.eff.org

some areas that are typically regulated on that level, but given the ease with which borders can be crossed in cyberspace, a legal structure that can impact a larger geographic entity will often be more effective.

(9) Even though the US has continued to dominate both access to cyberspace and the nature of online content, the Internet must inevitably be viewed at least on some level as a global communications medium. Given the fact that any particular moment persons may be connected to the internet from anywhere in the world and through servers located across the globe, international agreement and cooperation has become an essential component of any regulatory strategy. As the Internet continues to foster globalization and as nations move toward the identification of international baselines for certain key areas of the law, the prospects for international cooperation are good here.

(10) Code based change at various levels of the Internet architecture has emerged as potentially the single most powerful regulatory strategy available. Especially when combined with one or more of the other models, software solutions can have a dramatic impact in a setting that is in fact comprised solely of binary code. Yet even as caution must be exercised in this area so that the essential nature of cyberspace does not change, it must be recognized that code based changes in the online world have often been successfully countered by other code based changes. That means technology can be used circumvent other technologies.

(11) Private ordering continues to be set forth as a viable regulatory option by many stake holders and its potential effectiveness either by itself or in creative combination with other approaches should not be overlooked. It is in fact useful to identify two types of private ordering. The first, private architectural adjustment through the use of filtering, firewalls and other security measures- can serve a protective function for individuals and groups against unlawful or inappropriate activity. The second, private rule-making by networks, content providers and institutions, will typically dictate what others can and cannot do. While the former is appropriately viewed as

subcomponent of the broad architectural change model, the latter can generally be seen as a type of self-regulation.

(12) Whatever strategies or combination of strategies that are ultimately adopted, regulators must set forth guidelines that are clear, direct and understandable. Intellectual property laws, for example, have proven notoriously difficult for the average online user to comprehend and we should see that simple and straightforward rules are formulated for the benefit of all.

(13) In addition, regulatory approaches must be realistic. While this may seem inherently obvious, we have noted, for example, that the law has not truly come to grips with private personal copying since the advent of the Xerox machine and the widespread availability of audio taping and videotaping technology. Certain adjustments have been made, but most of the personal day-to-day copying that takes place in the privacy of an individual's own home remained subject to the vagaries of conflicting legal interpretation.

(14) As a related corollary, the importance of the implicit social contract in cyberspace must also be taken into account. Clear and realistic rules are an important beginning, but it must also be recognized that, on some level, our legal system is often based upon an implicit social contract. People must want to follow the law, and if they decide they no longer wish to d so, the implicit social contract breaks down. Particularly in certain cyber spaces, where law breaking is still very easy, steps must be taken to foster a spirit of cooperation between and among all online users.

(15) To this end, regulators must recognize and build on existing social norms. While there has been much debate in the legal and policy literature regarding the extent to which Internet norms can be pinpointed, most commentators agree that – at least for specific areas of the law and in particular cyber spaces – identifiable traditions and clear community standards exist. Examples of generally accepted activity that may have already influenced the development of the law in this regard include linking

without permission , a commitment to libertarian view of free speech rights, an ongoing consensus regarding a perceived right to remain anonymous and a broad acceptance of file sharing technology to create new digital copies of previously protected works. It is pertinent to note here that all these accepted norms in cyberspace among the entities constitute basic human rights in the physical world.

(16) In India regulatory norms related to privacy, defamation, copyright and trademarks need to be modified to meet the challenges posed by the Internet. There is no express provision guaranteeing right to privacy in Constitution or in any statutory enactment. Law relating to defamation is regulated under IPC and common law and our copyright law fails to take care of the new legal situations created by the Internet. Another way of dealing with the issues associated with cyberspace regulation may be considered under Information Technology Act, 2000, (IT Act) with suitable amendments. It is an enabling act and aims at promoting e-commerce. It provides no solutions to matters like privacy, defamation and copyright. IT Act may be suitably amended to include provisions for regulating privacy, defamation, copyright and trademarks.

(17) India may consider to have a separate legislation to control and regulate the collection and dissemination of personal data of netizens and in this regard it may adopt the data collection principles of OECD or it may follow the EU guidelines on data collection. Personal data now being treated as commodity and has become a billion dollar industry, this seems to be the appropriate approach.

(18) Copyright Act, 1957 must be suitable amended to meet the challenges of Internet medium and especially this must be done in the area of Digital Rights Management (DRM). As DRM may tilt the balance in favour of right holder, Sec.52 and Sec.53 have to be amended in such way that the copyright balance is maintained even in digital environment.

(19) Even though trademark law seems to be adequate to deal with the domain name problems in cyberspace, sometimes applications of the

provisions of the Trademark Act, 1999 may not be suitable to regulate cybersquatting and domain name abuse in cyberspace. The standards of interpretation that is used in the real space for trademarks may not be suitable for domain names of cyberspace.

(20) Keeping in view the concerns I have expressed about privacy, defamation, copyright, trademark and other grey areas of cyberspace and in order to avoid ambiguity and varied interpretation by judiciary these issues must be covered under a separate enactment , say, Internet Act or Cyberspace Transaction Act

(21) Ultimately, in the area of cyberspace regulation, there is no magic formula and quick fix. Particularly for certain intractable problems, solutions simply may not be imminent. In these cases, it is important to identify combinations of approaches that may serve to move things in the right direction. Compromises that may seem unacceptable now could become central features of such new approaches under one or more of the three major regulatory models – traditional national law, international agreement and code based change.

The Internet today is one of the great achievements of the modern era, and any attempt to adjust its realities for regulatory purposes must proceed slowly and with great caution. Perhaps the most important of all the inherent limits of our legal system is the rule of unintended consequences. Especially in light of the fact that cyberspace technology will inevitable continue to change, it is essential that we seek to avoid modifications that may have unanticipated effects.

Given the dramatic innovations we witnessed over the past fifteen years it is particularly difficult to predict how cyberspace might look down the road. Most agree that wireless access will become more prevalent, and that a range of smaller and lighter information appliances will enable people to connect more easily to networked environment. Indeed, if anything is certain, is the fact that we will continue to become even more interconnected in the future.

Beyond these basic certainties, however, a range of predictions abound. Prognosticators focusing on the technology have set forth dazzling scenarios that expand the limits of human potential. Those who focus on lifestyle envision an Internet that is so much part of our daily affairs that we no longer think of it as something separate and apart. At that point, many argue, there will be no such thing as cyberspace law because the online world will be virtually indistinguishable from the offline world. There will be no member separate Internet specialization in law and public policy, because every member of the legal profession will be an Internet lawyer and everyone engaged in public policy will be an Internet policy maker.

It does not matter how future internet technologies impact on our society in relation to social, cultural, economic and legal systems, the regulatory mechanism must provide for the promotion and protection of human rights. In the history of our civilizations the internet technologies have created a capacity in such a way that all of us are equal in at least expressing our views and opinions. Regulators should worry how technologies are being used by people rather than how these technologies work.