Temping: A tradition in transition  
Dr. Aisha M. Sheriff  
Dr. P. Nagesh  

Factors Affecting the Growth of Small Manufacturing Firms in Coimbatore City  
Dr. Ganapati  
R. Geetha Ramani  

A Study on Consumption Pattern of Preserved Foods in Satara District  
Vrushali Shah  
Dr. Sarang Bhola  

The Impact on Knowledge, Skill, Experience, Qualification and Culture in Merged Entities.  
James Thomas  

Global Identification of the Cyber Laws  
R. G. Pawar  
Dr. B. S. Sawant  

Communication and Promotion in Rural Markets  
Manoj Narwade  

CSR: A Strategic Management Tool of Pepsico India.  
Ms. Rashmi H.  
Ms. Subrata S.  

Implications of Information Technology and Its Impact in Organizational Values: A Study of Developing Countries  
Sambit Kumar Mishra  

Exploring cross cultural dimensions for hiring processes  
Anuha Shurke  
Dr. Malini Shurke  

Achieving Customer Satisfaction through Customer Experience Management  
Nazia Sultana  

Challenges of HRD in Public Sector Banks in the New Environment  
Dr. S. Husain Ashraf  

Relationship Marketing: A Mantra For Marketing Success  
Anurag Mittal  

A Peep into the Investment Climate of China and India  
Dr. P. Paramashivaiah  
Dr. Aravind S.  

Evolution of Private Labels in developing economies.  
Shilpa Kamath  

Employees Attitude towards Ethical orientation in HRM Practices: A Case Study  
Pankaj Tiwary  

Retaining an Employee A novel approach  
Dr. Ahmed Umar Khan  

Tourism: An avenue of Organised Retail Sector  
Sajid Alvi  
Ramkrishana Dikkatwar  

Mohsin R. Shaikh  

Green Marketing  
Dr. Jyotsna Haran  
Dr. Deepak Bhandari
ABOUT CMRD Journal of Management Research (CJMR)

The Philosophy: CMRD Journal of Management Research (CJMR) invites innovative and preferably research-based articles in any area of management. Practicing managers are welcome to submit data-based case studies for publication. All authors should aim at advancing existing thought and/or practices in the relevant field and hence should endeavour to be original and insightful. Submissions should indicate an understanding of the relevant literature and the contribution of the submissions to this body of research. Empirical articles should have an appropriate methodology and be able to relate their findings to the existing literature. Methodological articles must attempt to show how they further existing theory.

The review process: The review process followed by CJMR is systematic and thorough. Articles submitted to the journal are initially screened by the editor for relevance and overall quality as judged by the presentation of concepts, methodology and

Contents

02 Temping: A tradition in transition
Dr. Aisha M. Sheriff
Dr. P. Nagesh

08 Factors Affecting the Growth of Small Manufacturing Firms in Coimbatore City
Dr. Ganapati
R. Geetha Ramani

12 A Study on Consumption Pattern of Preserved Foods in Satara District
Vrushali Shah
Dr. Sarang Bhola

20 The Impact on Knowledge, Skill, Experience, Qualification and Culture in Merged Entities.
James Thomas

23 Global Identification of the Cyber Laws
R.G Pawar
Dr. B.S Sawant

32 Communication and Promotion in Rural Markets
Manoj Narwade

39 CSR: A Strategic Management Tool of Pepsico India.
Ms. Rashmi H.
Ms. Subhraja S.

47 Implications of Information Technology and Its Impact in Organizational Values: A Study of Developing Countries
Sambit Kumar Mishra

53 Exploring cross cultural dimensions for hiring processes
Anagha Shurke
Dr. Malini Shurke

59 Achieving Customer Satisfaction through Customer Experience Management
Nazia Sultanah

64 Challenges of HRD in Public Sector Banks in the New Environment
Dr. S. Husain Ashraf

69 Relationship Marketing: A Mantra For Marketing Success
Anurag Mittal

72 A Peep into the Investment Climate of China and India
Dr. P. Paramashivaiah
Dr. Arvind S

75 Evolution of Private Labels in developing economies.
Shilpa Kamath

TRUE COPY

Librarian,
Karmaveer Bhaurao Patil Institute of Management Studies & Research,
Satara.
Global Identification of the Cyber Laws

R.G. Pawar

Dr. ILS Sawant

Introduction:
Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of applying laws based on geographic boundaries. While these electronic communications play havoc with geographic boundaries, a new boundary, made up of the screens and passwords that separate the virtual world from the "real world" of atoms, emerges. This new boundary defines a distinct Cyberspace that needs and can create new law and legal institutions of its own. Territorially-based law-making and law-enforcing authorities find this new environment deeply threatening.

Established territorial authorities may yet learn to defer to the regulatory efforts of Cyberspace participants who care most deeply about this new digital trade in ideas, information, and services. Separated from doctrine tied to territorial jurisdictions, the new rules will emerge, in a variety of online spaces, to govern a wide range of new phenomena that have no clear parallel in the non-virtual world. These new rules will play the role of law by defining legal personhood and property, resolving disputes, and crystallizing collective conversations about core values.

In the today's era of rapid growth, Information technology is encompassing all walks of life all over the world. These technological developments have made the transition from paper to paperless transactions possible. We are now creating new standards of speed, efficiency, and accuracy in communication, which has become key tools for boosting innovations, creativity and increasing overall productivity. Computers are extensively used to store confidential data of political, social, economic or personal nature bringing immense benefit to the society.

Teritorial Borders

We take for granted a world in which geographical borders—lines or demarcating physical spaces—are of primary importance in determining legal rights and responsibilities: "All law is primitively territorial." Territorial borders, generally speaking, delineate areas within which different sets of legal rules apply. There has until now been a general correspondence between borders drawn in physical space (between nation states or other political entities) and borders in "law space." For example, if we were to superimpose a "law map" (delineating areas where different rules apply to particular behaviors) onto a political map of the world, the two maps would overlap to a significant degree, with clusters of homogenous applicable law and legal institutions fitting within existing physical borders, distinct from neighboring homogenous clusters.

The rapid development of Internet and Computer technology globally has led to the growth of new forms of transnational crime especially Internet related. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness and enactment of necessary legislation in all countries for the prevention of computer related crime. Globally Internet and Computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. This new boundary, which is made up of the screens and passwords, separate the "Cyber world" from the "real world" of atoms. Territorially based law-making and law-enforcing authorities find this new environment deeply threatening.

When Geographic Boundaries for Law Make Sense

Physical borders are not, of course, simply arbitrary creations. Although they may be based on historical accident, geographic borders for law make sense in the real world. Their relationship to the development and enforcement of legal rules is logically based on a number of related considerations.

Each community lives by its own law. As transport and media improve, transactions increase between distinct communities. As a result, conflicts tend to arise between the respective laws of these communities. For example, a judge may ask whether to apply the law of the forum community, or that of another community, in a case where one of the parties is from the other community or where a private transaction moves between the communities. In the middle ages, these communities were not necessarily territorial; they only became so with the modern advent of the nation-state.

The nation-state arose as geographers were mapping the world in co-ordinates of latitude and longitude. National law was then asserted as sovereign within territorial borders traced out in this geographic space. In the nineteenth century, von Savigny conceived of each set of legal relations as having its focal point in one such territory. For example, rights of real property could be seen as assuring the power of the owner of land to control trespass and like behaviours of any and all legal subjects relative to that land. Such property claims, von Savigny concluded, were subject to the law in effect at the situs of the land.

Von Savigny sought a method for choosing the same laws to govern the same legal claims, no matter where suit was brought or who brought it. His method may be encapsulated in the following three steps: First, determine the appropriate focal point, sometimes called a connecting factor or point of attachment, for each category of legal claim. Secondly, in order to know what points are appropriate in a given case, characterise (qualifier) each claim asserted in the case in terms of legal categories. Thirdly, localise the corresponding point of attachment in a given state whose law then applies to the claim at issue.

For von Savigny, there could be no interplay between characterisation (qualification) and localisation for a simple reason. He posited that legal relations developed inside, but without impacting on, geographic space.

*H G Pawar is Assistant Professor at Singhad Institute of Management, Pune.
**Dr. ILS Sawant is Director at KBP Institute of Management Science and Research, Satara.
For broad-ranging torts such as defamation or the infringement of intellectual property, the analysis is less simple. Nonetheless, the classic premise that geographic space is a fixed framework for conflicts analysis has not been questioned in the field of intellectual property. The Berne and Paris Conventions, and later treaties, impose the principle of national treatment supplemented by minimum rights, as well as the principle of the independence of rights. That is, foreign treaty claimants enjoy the same rights as nationals of a treaty country, the so-called protecting country, unless they are entitled to more extensive minimum rights, and the rights in one state do not depend on those in others. This approach corresponds to the classic conflicts rule in the field of torts: the law of the place of infringing acts governs resulting claims.

**Power.**

Control over physical space, and the people and things located in that space, is a defining attribute of sovereignty and statehood. Law-making requires some mechanism for law enforcement, which in turn depends (to a large extent) on the ability to exercise physical control over, and to impose coercive sanctions on, law-violators. For example, the U.S. government does not impose its trademark law on a Brazilian business operating in Brazil, at least in part because imposing sanctions on the Brazilian business would require assertion of physical control over those responsible for the operation of that business. Such an assertion of control would conflict with the Brazilian government’s recognized monopoly on the use of force over its citizens.

**Effects.**

The correspondence between physical boundaries and boundaries in "law space" also reflects a deeply rooted relationship between physical proximity and the effects of any particular behavior. That is, Brazilian trademark law governs the use of marks in Brazil because that use has a more direct impact on persons and assets located within that geographic territory than anywhere else. For example, the existence of a large sign over "Jones’ Restaurant" in Rio de Janeiro is unlikely to have an impact on the operation of "Jones’ Restaurant" in Oslo, Norway, for we may assume that there is no substantial overlap between the customers, or competitors, of these two entities. Protection of the former’s trademark does not probably should not affect the protection afforded the latter’s.

**Eigendom.**

We generally accept the notion that the persons within a geographically defined border are the ultimate source of law-making authority for activities within that border. The "consent of the governed" implies that those subject to a set of laws must have a role in their formulation. By virtue of the preceding considerations, a category of persons subject to a sovereign’s laws, and most explicitly affected by those laws, will consist primarily of individuals who are located in particular physical spaces. Similarly, allocation of responsibility among levels of government proceeds on the assumption that, for many legal problems, physical proximity between the responsible authority and those most directly affected by the law will improve the quality of decision making, and that is to determine the will of those individuals in physical proximity to one another.

**Lice.**

Physical boundaries are also appropriate for the delineation of "law space" in the physical world because they can give notice that the laws change when the boundaries are crossed. Proper boundaries have signposts that provide warning that we will be required, after crossing, to abide by different rules, and physical boundaries—lines on the geographical map—are generally well-equipped to serve this signpost function.

**The Absence of Territorial Borders in Cyberspace.**

Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.

The Net thus radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules. Cyberspace has no territorially-based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location: Messages can be transmitted from any physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another. The Net enables transactions between people who do not know, and in many cases cannot know, the physical location of the other party. Location remains vitally important, but only location within a virtual space consisting of the "addresses" of the machines between which messages and information are routed. The system is indifferent to the physical location of those machines, and there is no necessary connection between an Internet address and a physical jurisdiction.

Although a domain name, when initially assigned to a given machine, may be associated with a particular Internet Protocol address corresponding to the territory within which the machine is physically located (e.g., a "in" domain name extension), the machine may move in physical space without any movement in the logical domain name space of the Net. Or, alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location. Thus, a server with a "in" domain name may not necessarily be located in the India, a server with a " .com" domain name may be anywhere, and users, generally speaking, are not even aware of the location of the server that stores the content that they read. Physical borders no longer can function as signposts informing individuals of the obligations assumed by entering into a new, legally significant, place, because individuals are unaware of the existence of those borders as they move through virtual space.

The power to control activity in Cyberspace has only the most tenuous connections to physical location. Many governments first respond to electronic communications crossing their territorial borders by trying to stop or regulate that flow of information as it crosses their borders. Rather than deferring to efforts by participants in online transactions to regulate their own affairs, many governments establish trade barriers, seek to tax any border-crossing cargo, and respond especially sympathetically to claims that information coming into the jurisdiction might prove harmful to local residents. Efforts to stem the flow increase as online information becomes more important to local citizens. In particular, resistance to "transborder data flow" (TDF) reflects the concerns of
sovereign nations that the development and use of TDF's will undermine their 'informational sovereignty,' will negatively impact on the privacy of local citizens, and will upset private property interests in information. Even local governments in the United States have expressed concern about their loss of control over information and transactions flowing across their borders.

It is in this sense that laws of intellectual property are territorial. The category at the heart of the classic conflicts rule, the place of infringing acts, is territorial. In the nineteenth century, the meaning of this category seemed self-evident to courts considering infringement claims at home. They easily localised places where copyright works were put on stage or published, where trade marked goods were sold, and where patented inventions were used or made. Such acts took place where live performances, hard copies or products, or factories were found, on one side or the other of clearcut borders, inside a patchwork of national markets.

Unfortunately, the key category here, the place of infringing acts, can be doubly ambiguous. To start, before knowing what place that is, a court must localise the acts in question, but authorities differ about what law or laws provide terms in which to characterise infringing acts. In addition, the place of such acts can be extended backwards to that of preliminary acts, such as organising the infringement, or forwards to the place of damages. At the end of the twentieth century, the meaning of this place, once obvious in geographical space, is becoming impossible to pin down in cyberspace. The points where acts of infringement begin and end become indistinguishable as transactions cross multiple borders simultaneously in global, interactive networks.

This ambiguity arises out of the increasing efficacy of the media and technology. Legal relations develop within spaces in which, with increasing speed and power, subjects communicate with each other and control objects at a distance. To the extent that legal claims bear on communication and control itself, as they will in fields such as defamation and intellectual property, a principle of indeterminacy comes into play. Depending on what laws govern claimants' rights in such fields, their respective positions of power will change in what might be called social space, that is, in the relevant communication and control networks. Thus characterisation and localisation are not categorically independent of each other, but rather tied together to the extent that they impact on the values at stake in the overall resolution of any conflict of laws which they help to formulate. In these threshold inquiries to determine the places of infringing acts, the public policies underlying conflicts analysis, ultimately considerations of ordre public, already come into play. Since more powerful media accentuate the ambiguity of territoriality, it is to be expected that the Internet dramatises the policies at stake in localisation. In particular, in localising the place of the infringing act in one spot or another, a court might apply the law of one country or another throughout any global network. If the law of one country provides too little protection, or another too much protection, applying one or the other law can result in pirate havens or choke points for data flow in the network. For example, what law should govern transmitting raw data from a European database via the Internet to the United States or China? Suppose, on the one hand, that a court localises the relevant acts in the United States or China, where data is received but not strongly protected: then, to European eyes, pirates may find havens in these countries, from which data might be more or less freely retransmitted. Suppose, on the other hand, that a court localises inside *127 Europe all unauthorised transmissions of raw data from Europe: then a European law granting property rights in the data might apply to the transmissions, even to the United States or China. That choice of law might well choke off data flow or at points within the Internet that policies in these countries would still leave open.

Typically, while reasoning in terms of fixed territorial categories, courts vacillate considerably in localising infringing acts and choosing applicable laws.

1. The Trademark Example.

The question who should regulate or control Net domain names presents an illustration of the difficulties faced by territorially-based law-making. The engineers who created the Net devised a "domain name system" that associates numerical machine addresses with easier-to-remember names. Thus, an Internet Protocol machine address like "35.21.0.69" can be derived, by means of a lookup table, from "leland.stanford.edu." Certain letter extensions (".com," ".edu," ".org," and ".net") have developed as global domains with no association to any particular geographic area. Although the Net creators designed this system as a convenience, it rapidly developed commercial value, because it allows customers to learn and remember the location of particular Web pages or e-mail addresses. Currently, domain names are registered with specific parties who echo the information to "domain name servers" around the world. Registration generally occurs on a "first come, first served" basis, generating a new type of property akin to trademark rights, but without inherent ties to the trademark law of any individual country. Defining rights in this new, valuable property presents many questions, including those relating to transferability, conditions for ownership (such as payment of registration fees), duration of ownership rights, and forfeiture in the event of abandonment, however defined. Who should make these rules?

Consider the placement of a "traditional" trademark on the face of a World Wide Web page. This page can be accessed instantly from any location connected to the Net. It is not clear that any given country's trademark authorities possess, or should possess, jurisdiction over such placements. Otherwise, any use of a trademark on the net would be subject simultaneously to the jurisdiction of every country. Should a Web page advertising a local business in Illinois be deemed to infringe a trademark in Brazil just because the page can be accessed freely from Brazil? Large U.S. companies may be upset by the appearance on the Web of names and symbols that overlap with their valid U.S.-registered trademarks. But these same names and symbols could also be validly registered by another party in Mexico whose "infringing" marks are now, suddenly, accessible from within the United States. Upholding a claim of infringement or dilution launched by the holder of a U.S.-registered trademark, solely on the basis of a conflicting mark on the Net, exposes that trademark holder to claims from other countries when the use of their U.S.-registered mark on the Web would allegedly infringe a similar mark in those foreign jurisdictions.

2. Migration of Other Regulated Conduct to the Net.

Almost everything involving the transfer of information can be done online: education, health care, banking, the provision of intangible services, all forms of publishing, and the practice of law. The laws regulating many of these activities have developed as distinctly local and territorial. Local authorities certify teachers, charter banks with authorized "branches," and license doctors and lawyers. The law has in essence presumed that the activities
conducted by these regulated persons cannot be performed without being tied to a physical body or building subject to regulation by the territorial sovereign authority, and that the effects of those activities are most distinctly felt in geographically circumscribed areas. These distinctly local regulations cannot be preserved once these activities are conducted by globally dispersed parties through the Net. When many trades can be practiced in a manner that is unrelated to the physical location of the participants, these local regulatory structures will either delay the development of the new medium or, more likely, be superseded by new structures that better fit the online phenomena in question.

Any insistence on "reducing" all online transactions to a legal analysis based in geographic terms presents, in effect, a new "mind-body" problem on a global scale. We know that the activities that have traditionally been the subject of regulation must still be engaged in by real people who are, after all, at distinct physical locations. But the interactions of these people now somehow transcend those physical locations. The Net enables forms of interaction in which the shipment of tangible items across geographic boundaries is irrelevant and in which the location of the participants does not matter. Efforts to determine "where" the events in question occur are decidedly misguided, if not altogether futile.

A New Boundary for Cyberspace

Although geographic boundaries may be irrelevant in defining a legal regime for Cyberspace, a more legally significant border for the "law space" of the Net consists of the screens and passwords that separate the tangible from the virtual world. Traditional legal doctrine treats the Net as a more transmission medium that facilitates the exchange of messages sent from one legally significant geographical location to another, each of which has its own applicable laws.

Yet, trying to tie the laws of any particular territorial sovereignty to transactions on the Net, or even trying to analyze the legal consequences of Net-based commerce as if each transaction occurred geographically somewhere in particular, is most unsatisfying.

A. Cyberspace as a Place

Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the "real world."

Using this new approach, we would no longer ask the unanswerable question "where" in the geographical world a Net-based transaction occurred. Instead, the more salient questions become: What rules are best suited to the often unique characteristics of this new place and the expectations of those who are engaged in various activities there? What mechanisms exist or need to be developed to determine the content of those rules and the mechanisms by which they can enforced?

Answers to these questions will permit the development of rules better suited to the new phenomena in question, more likely to be made by those who understand and participate in those phenomena, and more likely to be enforced by means that the new global communications media make available and effective.

2. The Trademark Example.

The ultimate question who should set the rules for uses of names on the Net presents an apt microcosm for examining the relationship between the Net and territorial-based legal systems. There is nothing more fundamental, legally, than a name or identity—the right to legally recognized personhood is a predicate for the amassing of capital, including the reputational and financial capital, that arises from sustained interactions. The domain name system, and other online uses of names and symbols tied to reputations and virtual locations, exist operationally only on the Net. These names can, of course, be printed on paper or embodied in physical form and shipped across geographic borders. But such physical uses should be distinguished from electronic use of such names in Cyberspace, because publishing a name or symbol on the Net is not the same as intentional distribution to any particular jurisdiction. Instead, use of a name or symbol on the Net is like distribution to all jurisdictions simultaneously. Recall that the country-based domain names like "com," and "edu" lead to the establishment of online addresses on a global basis. And through such widespread use, the global domain names gained proprietary value. In this context, assertion by any local jurisdiction of the right to set the rules applicable to the "domain name space" is an illegitimate extra-territorial power grab.

Conceiving of the Net as a separate place for purposes of legal analysis will have great simplifying effects. For example, a global registration system for all domain names and reputationally significant names and symbols used on the Net would become possible. Such a Net-based regime could take account of the special claims of owners of strong global marks (as used on physical goods) and "grandfather" these owners' rights to the use of their strong marks in the newly opened online territory. But a Net-based global registration system could also fully account for the true nature of the Net by treating the use of marks on Web pages as a global phenomenon, by assessing the likelihood of confusion and dilution in the online context in which such confusion would actually occur, and by harmonizing any rules with applicable engineering criteria, such as optimizing the overall size of the domain name space.

A distinct set of rules applicable to trademarks in Cyberspace would greatly simplify matters by providing a basis to resist the inconsistent and conflicting assertions of geographically local prerogatives. If one country objects to the use of a mark on the Web that conflicts with a locally registered mark, the rebuttal would be that the mark has not been used inside the country at all, but only on the Web. If a company wants to know where to register its use of a symbol on the Net, or to check for conflicting prior uses of its mark, the answer will be obvious and cost effective: the designated registration authority for the relevant portion of the Net itself. If we need to develop rules governing abandonment, dilution, and conditions on uses of particular types of domain names and addresses, those rules—applicable specifically to Cyberspace—will be able to reflect the special characteristics of this new electronic medium.

The New Boundary is Real.

Treating Cyberspace as a separate "space" to which distinct laws apply should come naturally, because entry into this world of stored online communications occurs through a screen and (usually) a "password" boundary. There is a "placelessness" to Cyberspace because the messages accessed there are persistent and accessible to many people. You know when you are "there." No one accidentally strays across the border into Cyberspace. To be sure, Cyberspace is
because the Net has distinct characteristics, including an enhanced ability of the allegedly defamed person to reply, the rules o

defamation developed for the Net could take into account these technological capabilities—perhaps by requiring that an opportunity for reply be taken advantage of in lieu of monetary compensation for certain defamatory net-based messages. The distinct characteristics of the Net could also be taken into account when applying and adapting the "public figure" doctrine in context that is both global and highly compartmentalized and blurs the distinction between private and public spaces.

This requirement is infeasible when professional services are dispensed over the Net and potentially provided in numerous jurisdictions. Establishing certification regimes that apply only to such activities on the Net would greatly simplify matters. Such regulations would take into account the special features of Net-based professional activities like tele-medicine or global law practice by including the need to avoid any special risks caused by giving online medical advice in the absence of direct physical contact with a patient or by answering a question regarding geographically local law from a remote location. Using this approach, we could override the efforts of local school boards to license online educational institutions, treating attendance by students at online institutions as a form of "leaving home for school" rather than characterizing the offering of education online as prosecutable distribution of disfavored materials into potentially unwelcoming community that asserts local licensure authority.

3. Fraud and Antitrust.

Even an example that might otherwise be thought to favor the assertion of jurisdiction by a local sovereign—protection of local citizens from fraud and antitrust violations—shows the beneficial effects of a Cyberspace legal regime.

How should we analyze "markets" for antitrust and consumer protection purposes when the companies at issue do business online. Through the World Wide Web? Cyberspace could be treated as a distinct marketplace for purposes of assessing concentration and market power. Concentration in geographic markets would only be relevant in the rare cases in which such market power could be inappropriately leveraged to obtain power in online markets—for example by conditionally access to the net by local citizens on their buying services from a single company (such as a phone company) online. Claims regarding a right to access to particular online services, as distinct from claims to access particular physical pipelines, would remain tenable: long as it is possible to create a new online service instantly at a corner of an expanding online space. Consumer protection doctrines could also develop differently online—to take into account the fact that anyone reading an online ad is only a mouse click away from guidance from consumer protection agencies and discussion with other consumers.

Can Minnesota prohibit the establishment of a Ponzi scheme on a Web page physically based in the Cayman Islands but accessed by Minnesota citizens through the Net? Under the proposed new approach to regulation of online activities, the answer is clearly no. Minnesota has no special right to prohibit such activities. The state lacks enforcement power, cannot sho distractedly targeted effects, and does not speak for the community with the most legitimate claim to self-governance. But that does not mean that fraud might not be made "illegal" in at least large areas of Cyberspace. Those who establish and use online systems have

Global Identification of the Cyber Laws

not a homogenous place; groups and activities found at various online locations possess their own unique characteristics and distinctions, and each area will likely develop its own set of distinct rules. But the line that separates online transactions from our dealings in the real world is just as distinct as the physical boundaries between our territorial governments—perhaps more so.

Crossing into Cyberspace is a meaningful act that would make application of a distinct "law of Cyberspace" fair to those who pass over the electronic boundary. As noted, a primary function and characteristic of a border or boundary is its ability to be perceived by the one who crosses it. As regulatory structures evolve to govern Cyberspace-based transactions, it will be much easier to be certain which of those rules apply to your activities online than to determine which territorial-based authority might apply its laws to your conduct. For example, you would know to abide by the "terms of service" established by CompuServe or America Online when you are in their online territory, rather than guess whether Germany, or Tennessee, or the SEC will succeed in asserting their right to regulate your activities and those of the "placeless" online personae with whom you communicate.

Other Cyberspace Regimes

Once we take Cyberspace seriously as a distinct place for purposes of legal analysis, many opportunities to clarify and simplify the rules applicable to online transactions become available.

1. Defamation Law

Treating messages on the Net as transmissions from one place to another has created a quandary for those concerned about liability for defamation. Messages may be transmitted between countries with very different laws, and liability may be imposed on the basis of "publication" in multiple jurisdictions with varying standards. In contrast, the approach that treats the global network as a separate place would consider any allegedly defamatory message to have been published only "on the Net" (or in some distinct subsidiary area thereof)—at least until such time as distribution on paper occurs.

This re-characterization makes more sense. A person who uploads a potentially defamatory statement would be able more readily to determine the rules applicable to his own actions. Moreover, because the Net has distinct characteristics, including an enhanced ability of the allegedly defamed person to reply, the rules of defamation developed for the Net could take into account these technological capabilities—perhaps by requiring that the opportunity for reply be taken advantage of in lieu of monetary compensation for certain defamatory net-based messages. The distinct characteristics of the Net could also be taken into account when applying and adapting the "public figure" doctrine in a context that is both global and highly compartmentalized and blurs the distinction between private and public spaces.

2. Regulation of Net-Based Professional Activities.

The simplifying effect of "taking Cyberspace seriously" likewise arises in the context of regimes for regulating professional activities. As noted, traditional regulation insists that each professional be licensed by every territorial jurisdiction where she provides services.

This re-characterization makes more sense. A person who uploads a potentially defamatory statement would be able more readily to determine the rules applicable to his own actions. Moreover, because the Net has distinct characteristics, including an enhanced ability of the allegedly defamed person to reply, the rules of defamation developed for the Net could take into account these technological capabilities—perhaps by requiring that the opportunity for reply be taken advantage of in lieu of monetary compensation for certain defamatory net-based messages. The distinct characteristics of the Net could also be taken into account when applying and adapting the "public figure" doctrine in a context that is both global and highly compartmentalized and blurs the distinction between private and public spaces.
interest in preserving the safety of their electronic territory and preventing crime. They are more likely to be able to enforce their own rules. And, as more fully discussed below, insofar as a consensually based "law of the Net" needs to obtain respect and deference from local sovereigns, new Net-based law-making institutions have an incentive to avoid fostering activities that threaten the vital interests of territorial governments.

4. Copyright Law.

We suggest, not without some trepidation, that "taking Cyberspace seriously" could clarify the current intense debate about how to apply copyright law principles in the digital age. In the absence of global agreement on applicable copyright principles, the jurisdictional problems inherent in any attempt to apply territorially-based copyright regimes to electronic works simultaneously available everywhere on the globe are profound. As Jane Ginsburg has noted:

A key feature of the GII [Global Information Infrastructure] is its ability to render works of authorship pervasively and simultaneously accessible throughout the world.

The principle of territoriality becomes problematic if it means that posting a work on the GII calls into play the laws of every country in which the work may be received when... these laws may differ substantially.

Should the rights in a work be determined by a multiplicity of inconsistent legal regimes when the work is simultaneously communicated to scores of countries? Simply taking into account one country's laws, the complexity of placing works in a digital network is already daunting; should the task be further burdened by an obligation to assess the impact of the laws of every country where the work might be received? Put more bluntly, for works on the GII, there will be no physical territoriality... Without physical territoriality, can legal territoriality persist?

But treating Cyberspace as a distinct place for purposes of legal analysis does more than resolve the conflicting claims of different jurisdictions: It also allows the development of new doctrines that take into account the special characteristics of the online "place."

The basic justification for copyright protection is that bestowing an exclusive property right to control the reproduction and distribution of works on authors will increase the supply of such works by offering authors a financial incentive to engage in the effort required for their creation. But even in the "real world," much creative expression is entirely independent of this incentive structure, because the author's primary reward has more to do with acceptance in a community and the accumulation of reputational capital through wide dissemination than it does with the licensing and sale of individual copies of works. And that may be more generally true of authorship in Cyberspace; because authors can now, for the first time in history, deliver copies of their creations instantaneously and at virtually no cost anywhere in the world, one might expect authors to devise new modes of operation that take advantage of, rather than work counter to, this fundamental characteristics of the new environment. One such strategy has already begun to emerge: giving away information at no charge -- what might be called the "Netscape strategy" -- as a means of building up reputational capital that can subsequently be converted into income (e.g., by means of the sale of services). As Esther Dyson has written:

Controlling copies (once created by the author or by a third party) becomes a complex challenge. You can either control something very tightly, limiting distribution to a small, trusted group, or you can rest assured that eventually your product will find its way to a large nonpaying audience - if anyone cares to have it in the first place. ... Much chargeable value will be in certification of authenticity and reliability, not in the content. Branding, name, identity, and other marks of value will be important; so will security of supply. Customers will pay for a stream of information and content from a trusted source. For example, the umbrella of The New York Times sanctifies the words of its reporters. The content churned out by Times reporters is valuable because the reporters undergo quality-control, and because others believe them... The trick is to control not the copies of your work but instead a relationship with the customers: subscriptions or membership. And that's often what the customers want, because they see it as an assurance of a continuing supply of reliable, timely content.

A profound shift of this kind in regard to authorial incentives fundamentally alters the applicable balance between the costs and benefits of copyright protection in Cyberspace, calling for a reappraisal of long-standing principles. So, too, do other unique characteristics of Cyberspace severely challenge traditional copyright concepts. The very ubiquity of file "copying" -- the fact that one cannot access any information whatsoever in a computer-mediated environment without making a "copy" of that information -- implies that any simple-minded attempt to map traditional notions of "copying" onto Cyberspace transactions will have perverse results. Application of the "first sale" doctrine (allowing the purchaser of a copyrighted work to freely resell the copy she purchased) is problematic when the transfer of a lawfully owned copy technically involves the making of a new copy before the old one is eliminated, as is defining "fair use" when a work's size is indeterminate, ranging from (1) an individual paragraph sold separately on demand in response to searches to (2) the entire database from which the paragraph originates, something never sold as a whole unit.

Treating Cyberspace as a distinct location allows for the development of new forms of intellectual property law, applicable only on the Net, that would properly focus attention on these unique characteristics of this new, distinct place while preserving doctrines that apply to works embodied in physical collections (like books) or displayed in legally significant physical places (like theaters). Current debates about applying copyright law to the Net often do, implicitly, treat it as a distinct space, at least insofar as commercial copyright owners somewhat inaccurately refer to it as a "lawless" place. The civility of the debate might improve if everyone assumed the Net should have an appropriately different law, including a special law for unauthorized transfers of works from one realm to the other; we could, in other words, regulate the smuggling of works created in the physical world, by treating the unauthorized uploading of a copy of such works to the Net as infringement. This new approach would help promoters of electronic commerce focus on developing incentive-producing rules to encourage authorized transfers into Cyberspace of works not available now, while also reassuring owners of existing copyrights to valuable works that changes in the copyright law for the Net would not require changing laws applicable to distributing physical works. It would also permit the development of new doctrines of implied license and fair use that, as to works first created on the Net or imported with the author's permission, appropriately allow the transmission and copying necessary to facilitate their use within the electronic realm.
Whether Structure is Responsible for the Activity comes forward on the Net?

Even if we agree that new rules should apply to online phenomena, questions remain about who sets the rules and how they are enforced. We believe the Net can develop its own effective legal institutions.

Experience suggests that the community of online users and service providers is up to the task of developing a self-governance system. The current domain name system evolved from decisions made by engineers and the practices of Internet service providers. Now that trademark owners are threatening the company that administers the registration system, the same engineers who established the original domain name standards are again deliberating whether to alter the domain name system to take these new policy issues into account. Who has the ultimate right to control policy in this area remains unclear.

Every system operator who dispenses a password imposes at least some requirements as conditions of continuing access, including paying bills on time or remaining a member of a group entitled to use (e.g., students at a university). System operators (sysops) have an extremely powerful enforcement tool at their disposal to enforce such rules—banishment. Moreover, communities of users have marshaled plenty of enforcement weapons to induce wrongdoers to comply with local conventions such as rules against flaming, shunning, mailbombs, and more. And both sysops and users have begun explicitly to recognize that formulating and enforcing such rules should be a matter for principled discussion, not an act of will by whoever has control of the power switch.

While many of these new rules and customs apply only to specific, local areas of the global network, some standards apply through technical protocols on a nearly universal basis. And widespread agreement already exists about core principles of "netiquette" in mailing lists and discussion groups --although, admittedly, new users have a slow learning curve and the Net offers little formal "public education" regarding applicable norms. Dispute resolution mechanisms suited to this new environment also seem certain to prosper. Cyberspace is anything but anarchic; its distinct rule sets are becoming more robust every day.

Perhaps the most apt analogy to the rise of a separate law of Cyberspace is the origin of the Law Merchant—a distinct set of rules that developed with the new, rapid boundary-crossing trade of the Middle Ages. Merchants could not resolve their disputes by taking them to the local noble, whose established feudal law mainly concerned land claims. Nor could the local lord easily establish meaningful rules for a sphere of activity he barely understood, executed in locations beyond his control. The result of this jurisdictional confusion, arising from a then-novel form of boundary-crossing communications, was the development of a new legal system—Lex Mercatoria. The people who cared most about and best understood their new creation formed and championed this new law, which did not destroy or replace existing law regarding more territorially-based transactions (e.g. transferring land ownership). Arguably, exactly the same type of phenomenon is developing in Cyberspace right now.

Governments cannot stop electronic communications coming across their borders, even if they want to do so. Nor can they credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that travel electronically to many different nations; one nation's legal institutions should not, therefore, monopolize rule-making for the entire Net. Even so, established authorities likely will continue to claim that they must analyze and regulate the new online phenomena in terms of some physical locations. After all, the people engaged in online communications still inhabit the material world. And, so the argument goes, local legal authorities must have authority to remedy the problems created in the physical world by those acting on the Net. The rise of responsible law-making institutions within Cyberspace, however, will weigh heavily against arguments that would claim that the Net is "lawless" and thus tie regulation of online trade to physical jurisdictions. As noted, sysops acting alone or collectively have the power of banishment to control wrongful actions online. Thus, for online activities that minimally impact the vital interests of sovereigns, the self-regulating structures of Cyberspace seem better suited than local authorities to deal with the Net's legal issues.

The Trademark Example

In order for the domain name space to be administered by a legal authority that is not territorially based, new law-making institutions will have to develop. Many questions that arise in setting up this system will need answers—decisions about whether to create a new top level domain, whether online addresses belong to users or service providers, and whether one name impermissibly interferes with another, thus confusing the public and diluting the value of the pre-existing name. The new system must also include procedures to give notice in conflicting claims, to resolve these claims, and to assess appropriate remedies (including, possibly, compensation) in cases of wrongful use. If the Cyberspace equivalent of eminent domain develops, questions may arise over how to compensate individuals when certain domain names are destroyed or redeployed for the public good of the Net community. Someone must also decide threshold membership issues for Cyberspace citizens, including how much must disclose (and to whom) about their real-world identities to use e-mail addresses and domain names for commercial purposes. Implanted throughout this discussion is the recognition that these rules will only be meaningful and enforceable if Cyberspace citizens view whomever makes these decisions as a legitimate governing body.

Experience suggests that the community of online users and service providers is up to the task of developing a self-governance system. The current domain name system evolved from decisions made by engineers and the practices of Internet service providers. Now that trademark owners are threatening the company that administers the registration system, the same engineers who established the original domain name standards are again deliberating whether to alter the domain name system to take these new policy issues into account. Who has the ultimate right to control policy in this area remains unclear.

Every system operator who dispenses a password imposes at least some requirements as conditions of continuing access, including paying bills on time or remaining a member of a group entitled to use (e.g. students at a university). System operators (sysops) have an extremely powerful enforcement tool at their disposal to enforce such rules—banishment. Moreover, communities of users have marshaled plenty of enforcement weapons to induce wrongdoers to comply with local conventions such as rules against flaming, shunning, mailbombs, and more. And both sysops and users have begun explicitly to recognize that formulating and enforcing such rules should be a matter for principled discussion,
not an act of will by whoever has control of the power switch.

While many of these new rules and customs apply only to specific, local areas of the global network, some standards apply through technical protocols on a nearly universal basis. And widespread agreement already exists about core principles of "netiquette" in mailing lists and discussion groups—although, admittedly, new users have a slow learning curve and the Net offers little formal "public education" regarding applicable norms. Dispute resolution mechanisms suited to this new environment also seem certain to prosper. Cyberspace is anything but anarchic; its distinct rule sets are becoming more robust every day.

Perhaps the most apt analogy to the rise of a separate law of Cyberspace is the origin of the Law Merchant—a distinct set of rules that developed with the new, rapid boundary-crossing trade of the Middle Ages. Merchants could not resolve their disputes by taking them to the local noble, whose established feudal law mainly concerned land claims. Nor could the local lord easily establish meaningful rules for a sphere of activity he barely understood, executed in locations beyond his control. The result of this jurisdictional confusion, arising from a then-novel form of boundary-crossing communications, was the development of a new legal system—Lex Mercatoria. The people who cared most about and best understood their new creation formed and championed this new law, which did not destroy or replace existing law regarding more territorially-based transactions (e.g. transferring land ownership). Arguably, exactly the same type of phenomenon is developing in Cyberspace right now.

Governments cannot stop electronic communications coming across their borders, even if they want to do so. Nor can they credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that travel electronically to many different nations; one nation's legal institutions should not, therefore, monopolize rule-making for the entire Net. Even so, established authorities likely will continue to claim that they must analyze and regulate the new online phenomena in terms of some physical locations. After all, the people engaged in online communications still inhabit the material world. And, so the argument goes, local legal authorities must have authority to remedy the problems created in the physical world by those acting on the Net. The rise of responsible law-making institutions within Cyberspace, however, will weigh heavily against arguments that would claim that the Net is "lawless" and thus tie regulation of online trade to physical jurisdictions. As noted, sysops acting alone or collectively have the power of banishment to control wrongful actions online. Thus, for online activities that minimally impact the vital interests of sovereigns, the self-regulating structures of Cyberspace seem better suited than local authorities to deal with the Net's legal issues.

Local Authorities, Foreign Rules: Reconciling Conflicts

What should happen when conflicts arise between the local territorial law (applicable to persons or entities by virtue of their location in a particular area of physical space) and the law applicable to particular activities on the Net? The doctrine of "comity"—as well as principles applied when delegating authority to self-regulatory organizations, provides us with guidance for reconciling such disputes.

The doctrine of comity, in the Supreme Court's classic formulation, is "the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protections of its law."

It arose as an attempt to mitigate some of the harsher features of a world in which lawmaking is an attribute of control over physical space but in which persons, things, and actions may move across physical boundaries, and it functions as a constraint on the strict application of territorial principles that attempts to reconcile "the principle of absolute territorial sovereignty [with] the fact that intercourse between nations often demand[s] the recognition of one sovereign's lawmaker acts in the forum of another." In general, comity reflects the view that those who care more deeply about and better understand the disputed activity should determine the outcome. Accordingly, it may be ideally suited to handle, by extension, the new conflicts between the a-territorial nature of cyberspace activities and the legitimate needs of territorial sovereigns and of those whose interests they protect on the other side of the cyberspace border. This doctrine does not disable territorial sovereigns from protecting the interests of those individuals located within their spheres of control, but it calls upon them to exercise a significant degree of restraint when doing so.

Local officials handling conflicts can also learn from the many examples of delegating authority to self-regulatory organizations. Churches are allowed to make religious law despite the seeming contradiction of a sovereign deferring to the authority of those who are not its own subjects, such a policy makes sense, especially in light of the underlying purposes of both doctrines. Comity and delegation represent the wise conservation of governmental resources and allocate decisions to those who most fully understand the special needs and characteristics of a particular "sphere" of being. Although Cyberspace represents a new sphere that cuts across national boundaries, the fundamental principle remains. If the sysops and users who collectively inhabit and control a particular area of the Net want to establish special rules to govern conduct there, and if that rule set does not fundamentally impinge upon the vital interests of others who never visit this new space, then the law of sovereigns in the physical world should defer to this new form of self-government.

Internal Diversity

One of a border's key characteristics is that it slows the interchange of people, things, and information across its divide. Arguably, distinct sets of legal rules can only develop and persist where effective boundaries exist. The development of a true "law of Cyberspace," therefore, depends upon a dividing line between this new online territory and the non-territorial world. Our argument so far has been that the new sphere online is cut off, at least to some extent, from rule-making institutions in the material world and requires the creation of a distinct law applicable just to the online sphere.

But we hasten to add that Cyberspace is not, behind that border, a homogeneous or uniform territory behind that border, where information flows without further impediment. Although it is meaningless to speak of a French or Armenian portion of Cyberspace, because the physical borders dividing French or Armenian territory from their neighbors cannot generally be mapped onto the flow of information in Cyberspace, the Net has other kinds of internal borders delineating many distinct internal locations that slow or block the flow of information.

the Net has other kinds of internal borders delineating many distinct
internal locations that slow or block the flow of information. Distinct names and (virtual) addresses, special passwords, entry fees, and visual cues—software boundaries—can distinguish subsidiary areas from one another.

The hope for self-government today lies not in relocating sovereignty but in dispersing it. The most promising alternative to the sovereign state is not a cosmopolitan community based on the solidarity of humankind but a multiplicity of communities and political bodies—some more extensive than nations and some less—among which sovereignty is diffused. Only a politics that disperses sovereignty both upward [to transnational institutions] and downward can combine the power required to rival global market forces with the differentiation required of a public life that hopes to inspire the allegiance of its citizens. . . . If the nation cannot summon more than a minimal commonality, it is unlikely that the global community can do better, at least on its own. A more promising basis for a democratic politics that reaches beyond nations is a revitalized civic life nourished in the more particular communities we inhabit.

The ability of inhabitants of Cyberspace to cross borders at will between legally significant territories, many times in a single day, is unsettling. This power seems to undercut the validity of developing distinct laws for online culture and commerce. How can these rules be "law" if participants can literally turn them on and off with a switch? Frequent online travel might subject relatively mobile human beings to a far larger number of rule sets than they would encounter traveling through the physical world over the same period. Established authorities, contemplating the rise of a new law applicable to online activities, might object that we cannot easily live in a world with too many different sources and types of law, particularly those made by private (non-governmental) parties, without breaching confusion and allowing anti-social actors to escape effective regulation.

But the speed with which we can cross legally meaningful borders or adopt and then shed legally significant roles should not reduce our willingness to recognize multiple rule sets. Rapid travel between spheres of being does not detract from the distinctiveness of the boundaries, as long as participants realize the rules are changing. Nor does it detract from the appropriateness of rules applying within any given place, any more than changing commercial or organizational roles in the physical world detracts from a person's ability to obey and distinguish rules as a member of many different institutional affiliations and to know which rules are appropriate for which roles. Nor does it lower the enforceability of any given rule set within its appropriate boundaries, as long as groups can control unauthorized boundary crossing of groups or messages. Alternating between different legal identities many times during a day may confuse those for whom cyberspace remains an alien territory, but for those for whom cyberspace is a more natural habitat in which they spend increasing amounts of time it may become second nature. Legal systems must learn to accommodate a more mobile kind of legal person.

Conclusion

Clear boundaries make law possible, encouraging rapid differentiation between rule sets and defining the subjects of legal discussion. New abilities to travel or exchange information rapidly across old borders may change the legal frame of reference and require fundamental changes in legal institutions. Fundamental activities of lawmaking—accommodating conflicting claims, defining property rights, establishing rules to guide conduct, enforcing those rules, and resolving disputes—remain very much alive within the newly defined, intangible territory of Cyberspace. At the same time, the newly emerging law challenges the core idea of a current law-making authority—the territorial nation state, with substantial but legally restrained powers.

If the rules of Cyberspace thus emerge from consensually based rule sets, and the subjects of such laws remain free to move among many differing online spaces, then considering the actions of Cyberspace's system administrators as the exercise of a power akin to "sovereignty" may be inappropriate. Under a legal framework where the top level imposes physical order on those below it and depends for its continued effectiveness on the inability of its citizens to fight back or leave the territory, the legal and political doctrines we have evolved over the centuries are essential to constrain such power. In that situation, where exit is impossible, costly, or painful, then a right to a voice for the people is essential. But when the "persons" in question are not whole people, when their "property" is intangible and portable, and when all concerned may readily escape a jurisdiction they do not find empowering, the relationship between the "citizen" and the "state" changes radically. Law, defined as a thoughtful group conversation about core values, will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically-defined territories.

The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, places, and things found there. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world. For example, the law of the Net must deal with persons who "exist" in Cyberspace only in the form of an email address and whose purported identity may or may not accurately correspond to physical characteristics in the real world. In fact, an e-mail address might not even belong to a single person. Accordingly, if Cyberspace law is to recognize the nature of its "subjects," it cannot rest on the same doctrines that give geographically based sovereign jurisdiction over "whole," locatable, physical persons. The law of the Net must be prepared to deal with persons who manifest themselves only by means of a particular ID, user account, or domain name.

Reference:

- Dr. Farooq Ahmad, "Cyber Law in India", Pioneer Books, Page 27 to 32.
- Vaishali Bhagwat, "Law of Cyber Crimes in India".
- Information Technology Act, 2000 A contractual Perspective by Devadatt Kamat.