JOURNAL OF LAW AND SOCIETY
VOLUME 30, NUMBER 2, JUNE 2003
ISSN: 0263-323X, pp. 187–216

Regulation and Rights in Networked Space

ANDREW D. MURRAY*

The Internet is often described as inherently free from regulation; a space where freedoms and liberties are guaranteed by the design of the network environment. The naivety of this view has, however, been exposed by commentators such as Shapiro, Reidenberg, and Lessig who have clearly demonstrated the inherent regulability of networked space. The question no longer is: can networked space be regulated? but rather, how and by whom is it regulated? This paper examines the regulation of rights in networked space. Property rights and rights to free speech, or free expression, are examined in relation to a number of issues that have emerged in the networked environment, or cyberspace. Its aim is to examine whether the embryonic regulatory structure of cyberspace, which has the advantage of starting with a completely clean slate, is sufficiently sympathetic to the unique qualities of this fledgling jurisdiction.

INTRODUCTION

This paper examines the rules and institutional structures through which the peculiar tensions between proprietary rights and the right of free expression in cyberspace are mediated. It follows the positivistic approach to rights advocated by among others Ralph Beddard in his book *Human Rights and Europe*,[1] and focuses upon the rivalous nature of these rights.[2] The central

* *Law Department and Media@LSE, London School of Economics and Political Science, Houghton Street, London, WC2A 2AE, England*

Thanks are due, with the usual disclaimer, to Rachel Miles, Colin Scott, Dan Paré, Mathias Klang, Robin Mansell, and the participants of the Domain Names session at the BILETA Annual Conference 5–6 April 2002, Vrije Universiteit, Amsterdam.

1 R. Beddard, *Human Rights and Europe* (1993).
2 Often the exercise of basic moral rights will bring the actor into direct conflict with the basic moral rights of another. For example, if you choose, as part of a protest, to occupy my property, I may use my right to peaceful enjoyment of my possessions to curtail your right to free expression by having you removed.

question is whether the interplay between the rules for allocating domain names and the structures for mediating disputes is causing the importation of unsuitable concepts such as a unitary property right into cyberspace jurisprudence.

PROPRIETARY RIGHTS IN DOMAIN NAMES

The vexed question of the legal status of an Internet domain name[3] has engaged many legal academics and practitioners since Joshua Quittner registered, without any prior proprietary interest, the domain name *mcdonalds.com* in July 1994.[4] The literature analysing this issue may be classified as falling within one of three categories. The first comprises analyses which focus upon propertization of the domain name system (DNS) while neglecting any normative analysis of the proprietary nature of domain names.[5] These direct their attention to particular instances where one party is in active dispute with another over a domain name. They focus upon the tensions arising from the dichotomy between the international and unclassified nature of domain names as opposed to the domestic, classified nature of the trademark system. These analyses fail, though, to question the normative basis of such disputes and, in particular, the issue of whether a property right may be asserted over a domain name. The second category encompasses analyses which review the normative role of a domain name with regard to the underlying addressing system of

3 The domain name system (DNS) facilitates the ability of users to navigate the World Wide Web (WWW). It does so with the aid of two components; the domain name and its corresponding Internet Protocol (IP) number. A domain name is a unique address or identifier of a single page of text or other digital information contained on the WWW, such as <itlaw.org.uk>. An IP number is the unique underlying numeric address, such as 81.21.68.22.

4 J. Quittner, 'Billions Registered' *Wired*, 10 October 1994. Available at: <http://www.wired.com/wired/archive/2.10/mcdonalds.html> (visited 5 February 2003); J. Quittner, 'What's in a Name?' *Time*, 31 August 1998.

5 A non-exhaustive list of such analyses include: C. Waelde, 'Trade Marks and Domain Names: There's a lot in a Name' in *Law and the Internet a Framework for Electronic Commerce*, eds. L. Edwards and C. Waelde (2000); A. Murray, 'Internet Domain Names: The Trade Mark Challenge' (1998) 6 *International J. of Law and Information Technology* 285; I. Azmi, 'Domain Names and Cyberspace: the Application of Old Norms to New Problems' (2000) 81 *International J. of Law and Information Technology* 193; S. Abel, 'Trademark Issues in Cyberspace: The Brave New Frontier' (1999) 5 *Michigan Telecommunications and Technology Law Rev.* 91; R. Tucker, 'Information Superhighway Robbery: The Tortious Misuse of Links, Frames, Metatags, and Domain Names' (1999) 4 *Virginia J. of Law and Technology* 8; M. Halpern and A. Mehrotra, 'From International Treaties to Internet Norms: The Evolution of International Trade Mark Disputes in the Internet Age' (2000) 21 *University of Pennsylvania J. of International Economic Law* 523.

the Internet.[6] Such analyses generally view the key conflicts between the trademark system and the DNS as being centred upon the unique role of a domain name as both an addressing protocol and a 'badge' or identifier.[7] Rather than adopting the conflicting values approach characteristic of the first category, papers focusing on this aspect of domain naming generally direct their attention to the 'fit' between trademark law as developed in real-space and the use of domain names in the electronic realm. These commentaries differ from those in the first category as they address the normative basis of the DNS. Nevertheless, this second approach also neglects to give sufficient consideration to issues pertaining to property rights in domain names and propertization of the DNS.[8]

The focus of the third category is the legal basis of domain names and the DNS. This nascent socio-legal analysis is most clearly exemplified by the work of Milton Mueller.[9] He argues that 'control of the DNS root[10] is being used to create new and expanded (property) rights to names', and that these rights are 'often stronger than ... traditional legal rights in names.'[11] Mueller contends there is no natural property interest in the domain name space, but that a synthetic proprietary interest has been engineered by trademark holders through the actions of the World Intellectual Property Organisation (WIPO),[12] and is being enforced by the Internet Corporation for Assigned Names and Numbers (ICANN) through its Uniform Dispute Resolution Procedure (UDRP).[13] The basis of his argument is that proprietary rights,

6 D. Burk, 'Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks' (1995) 1 *Richmond J. of Law and Technology* 1; M. Tanner, 'Trademarks, Internet Domain Names, and the NSI: How Do We Fix A System That Is Already Broken?' (1998) 3(2) *J. of Technology, Law and Policy* 2.

7 In real space we differentiate between these roles. In general, names are particular emblems used to establish or designate identity; addresses are emblems designating location.

8 This category of analysis may thus be characterized as examining the technical norms of domain names, but failing to address the legal norms. Analyses in the third category address the legal norms.

9 M. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (2002) ch. 11. See, also, D. Dolkas and S. Menser, 'Is A Domain Name ''Property''?' *Gray Carey Articles of Interest*. Available at: <http://www.gcwf.com/gcc/GrayCary-C/News–Arti/Articles/112000.1.doc_cvt.htm> (visited 5 February 2003); C. Soares, 'Are Domain Names Property? The Sex.com Controversy' 2001 *Duke Law and Technology Rev.* Available at: <http://www.law.duke.edu/journals/dltr/articles/2001dltr0032.html> (visited 5 February 2003).

10 For a discussion of the DNS Root, see n. 67 below.

11 Mueller, op. cit., n. 9, p. 228.

12 These rights have been created through the WIPO Internet Domain Name Processes. *Final Report of First Process* 30 April 1999 (Publication No. 439) available at: <http://wipo2.wipo.int/process1/report/finalreport.html> (visited 5 February 2003); *Final Report of Second Process* 3 September 2001 (Publication No. 843) available at: <http://wipo2.wipo.int/process2/report/html/report.html> (visited 5 February 2003). See, also, Mueller, id., pp. 228–31.

13 id., pp. 232–4. The UDRP is analysed in depth below.

being the exclusive right to control how and by whom a particular thing may be used, create controlled space. On the one hand this controlled space may be tangible, as in the case of physical property; alternatively it may be intangible, manifesting itself as 'controlled vocabulary'. For example, if we think of trademark rights, we find that a proprietary interest in a particular image, phrase or sound creates a controlled vocabulary. The latter presupposes an authority to determine precise associations between terms (or images or sounds, and so on) and entities. Mueller argues this is anathema to the original aims of the DNS. According to this view, creating a controlled vocabulary through the use of proprietary interests produces a subjective evaluation of words which establishes a false value in domain names. To take an example, if one compares domain names with street addresses, we see that there is little economic value in the latter as they are an objective identifier of location (uncontrolled or free vocabulary), whereas in the DNS the creation of a controlled vocabulary has produced extensive economic value in domain names. Mueller avers that the creation of a controlled vocabulary in domain names is founded on several false assumptions pertaining to the use of domain names which prior to the process of propertiziation within the DNS did not apply.[14] He believes that the current actions of WIPO, ICANN, and the trademark holders is counter-intuitive to the processes of the DNS. To use his words, 'to turn domain names into a controlled vocabulary is like pushing a heavy rock uphill. One must constantly work against nature.'[15]

The dominant theme underlying Mueller's argument is that the application of property rights to domain names runs counter to the natural order of things. However, this is not a positive argument against the creation of a property structure in the DNS. Property theory is based upon social order and has little to do with natural order. Proprietary interests create structures of control and value whereas the natural order is an order of freedom. This is most clearly illustrated by the Hegelian principle that property is the embodiment of personality as recognized by others.[16] Hegel believed that the moral and political relations of individuals stemmed from their rights to property and that property ownership was a reflection of our social culture. Hegel's theory of property thus provides a complex social tableau against which to view the development and application of proprietary rights. In Hegelian theory, the act of taking property is achieved by 'embodiment by projection'.[17] This is realized by taking occupancy of the property through possession, labelling or physical development of the property. The key requirement of occupancy is that it can signal to another that this property is in the control of the individual. For Hegel, property is an

14 id., pp. 246–7.
15 id., p. 253.
16 G.W.F. Hegel, *Philosophy of Right* (1821, trans. S. Dyde, 1996).
17 See S.R. Munzer, *A Theory of Property* (1990) 67–70.

'intersubjective concept': it cannot exist without persons to recognize the control of the 'owner' of the property.[18] Occupancy classically is modelled using Locke's labour theory: this prescribes that land in its natural state is ownerless and that property rights arise through patterns of positive possession and the injection of labour.[19] Physical development of the property signals occupancy. An alternative to the labour model is the registration model used in the creation and management of intangible properties. As intangibles cannot be physically developed or possessed, we utilize registration as a proxy of possession. This can be seen clearly in the patents system wherein the act of registration signals possession.

The Hegelian model of social projection is not the only model used to describe property rights. Alternatives, such as the economic model, exist.[20] Whichever theory you subscribe to, property creates structures of control and value. This runs counter to the basic laws of nature in which things are in an unowned state. Mueller's argument that the application of property rights to domain names runs counter to the natural order of things is therefore not a positive argument against the creation of a property structure in the DNS. To argue such a position one must establish that the DNS does not fit within the established models of property theory.[21]

1. Modelling domain names

Munzer puts forward a 'pluralist theory of property' based on his thesis that a satisfactory theory of property should include some 'principle that recognizes the moral import of actions that affect persons' happiness, welfare, preference-satisfaction or the like.'[22] His theory rests upon three principles: (i) utility and efficiency, (ii) desert based upon labour and (iii) justice and equality. By examining the application of each of these principles to the DNS we can determine whether regarding the DNS as a system of property rights is consistent with property theory.

18 id., p. 69.

19 J. Locke, *Two Treatises of Government* (1694) part II, para. 32.

20 Modern free-market economies may be categorized as private-property economies. These are systems in which the means of production are mostly privately owned and the market performs distributive functions. The basis of such economies may be found in the principle of excludability. The right to exclude access to property allows for control of that property and control allows for the creation of a market in rights and things. See, further, G. Calabresi and A. Melamed, 'Property Rules, Liability Rules and Inalienability: One View of the Cathedral' (1972) 85 *Harvard Law Rev.* 1089; J. Coleman, *Risks and Wrongs* (1992).

21 In the clearest judicial opinion to date, Judge Ware classifies a domain name as an intangible property right. See *Kremen* v. *Cohen* 99 F Supp 2d 1168 (2000), at 1173. See, also, *Umbro International Inc* v. *3263851 Canada Inc* 3 February 1999, Virginia State Court, unreported, available at: <http://www.alston.com/docs/Articles/199709/umbrodns.htm> (visited 5 February 2003).

22 Munzer, op. cit., n. 17, p. 3.

The principle of utility and efficiency requires that property rights should be allocated so as to maximize utility and efficiency regarding the use, possession, and transfer of things.[23] This principle is designed to ensure maximum individual preference-satisfaction, while preserving the interests of the community. The DNS clearly fulfils this principle. A failure to recognize property in domain names would lead to disutility both on an individual and community level and would reduce efficiency within cyberspace. A lack of utility on the individual level would occur as individuals would find it impractical to develop a web presence (use) and impossible to control access to their personal web space (possession).[24] Although the Internet could function without creating a proprietary interest in domain names, navigation using underlying Internet Protocol identifiers, with their complex mathematical base, would render the development of a rich tapestry of content such as the World Wide Web unimaginable. Individuals and corporations would not have invested in web content were it not for the ability of domain names to act as a badge of possession and control. Recognizing property in the DNS fulfilled individual utility, or in Munzer's words, provided individual preference-satisfaction. In doing so, it also allowed for maximization of overall utility, and it did so with the least cost to the community as a whole, thus providing maximum available efficiency.[25]

The second principle, that of desert based upon labour, is derived from traditional Lockean principles. Locke believed that the productive capacity of human labour increased the supply of goods available for consumption and that therefore the expenditure of labour on the production of such useful goods should be rewarded through private property.[26] Munzer modifies Locke's model and suggests a qualified labour-desert principle. This provides for private property to reward labour where this does not impinge on the rights of others, the process of acquisition, post-acquisition changes, restriction on transfer or general scarcity.[27] Applying Munzer's model to the DNS, we see that cyberspace may be seen as a largely unowned domain that parallels the state of nature. Individuals may stake their claim for a portion of this dimension of the electronic realm by registering their interest in the form

23 id., p. 4.

24 On access rights see the case of *eBay* v. *Bidders Edge* 100 F. Supp. 2d 1058 (2000).

25 The 'Domain Name Rush' of the mid 1990s may be seen as the modern equivalent of the land rushes of the nineteenth century. They provide for an efficient and highly incentivized system to invite the development of under-developed property. See, further, J. Umbeck, *Theory of Property Rights With Applications to the California Gold Rush* (1982).

26 This approach may be seen in Locke, op. cit., n. 19, particularly at part II, paras. 25, 32, 34. This should be contrasted with his earlier view seen in *Essays on the Law of Nature* (1676) in which he viewed the competition for human resources as a zero sum game (see essay VIII).

27 Munzer, op. cit., n. 17, p. 5.

of a domain name.[28] The registration process publicizes the interest of the individual in a manner that is similar to taking possession. That said, identification of the injection of labour is more problematic. Commentators who are sympathetic to the labour-reward model may contend that the development of a web presence based upon a domain name amounts to an injection of labour. This assumption, though, is incorrect. Firstly, the content of the web page is transferable and is not directly linked to a domain name. Secondly, it may be claimed that a proprietary interest in a domain name is established upon registration of the name, rather than upon its application to specific content.[29] The injection of labour may, however, be found at the stage of creating the domain name. As with the development of a trademark, the development of a domain name involves at least some limited degree of creative effort. It is here that a domain name is quite dissimilar to a street address. Whereas the latter is merely allocated to the recipient, a domain name is created by the registrant. Therefore to classify a domain name as merely an addressing or location tool misapprehends the subjective element of the creation process. Provided that one accepts the efficacy of a frontier metaphor to conceptualize cyberspace, it may be established that the labour-desert principle is fulfilled.

The final principle calls for justice and equality in the property system. Domain name holdings are, as with all property, unequal in their individual holding. Corporations tend to replicate trade names and marks in several languages whereas individuals tend to register a single domain name.[30] This is acceptable within the principle of justice and equality provided everyone has a minimum amount of property and the inequalities do not undermine a fully human life in society.[31] Although many netizens[32] do not possesses a domain name registration, access to the DNS is open to all and is extremely inexpensive: any netizen wishing to register may do so.[33] The first requirement of justice and equality is therefore fulfilled: any individual

28 The author recognizes that this approach draws on a frontier metaphor to conceptualize cyberspace. This social metaphor is a common theme in much Internet-related research. However, the monocultural roots of this notion do not resonate well outside of North America. Some authors have suggested that it provides ideological expression to the interests of an emerging digital elite. See D. Neice, 'Cyberspace and Social Distinctions: Two Metaphors and a Theory' in *Inside the Communication Revolution: Evolving Patterns of Social and Technical Interaction*, ed. R. Mansell (2002).

29 *Kremen* v. *Cohen*, op. cit., n. 21, p. 1169.

30 The Coca-Cola Company, for instance, owns and operates many domain names including cocacola.com, sprite.com, dietcoke.com, and fanta.com. The author owns and operates a single domain name.

31 Munzer, op. cit., n. 17, p. 5.

32 Netizen is the universally accepted term for a citizen of the Internet.

33 Currently one UK registrar is offering registration for as little as £3.75 per annum. See <http://www.lowcostnames.co.uk/> (visited 3 February 2003).

has full and unhindered access to a minimum amount of property.[34] The second requirement, that inequalities do not undermine a fully human life in society, forms the basis of the analysis which takes place in the second part of this paper. Mueller contends that the creation of property in the DNS has led to such an unequal distribution of property that many netizens are effectively deprived of the ability to fully interact with cyber-society.[35] The purpose of this paper, at least in part, is to analyse this contention with particular reference to the conflict between the property basis of the DNS with the ability of netizens to engage in free speech within cyberspace.

A RIGHT TO FREE EXPRESSION?

As we begin the new millennium, early enthusiasm concerning the free speech enhancing potential of the electronic domain is beginning to fade. It is becoming clear that self-publication is only tolerated so far as deemed acceptable by regulators and the wider community. Shapiro draws attention to two methodologies of control which restrict free expression in networked space. The first, *controlling speech*, refers to direct regulatory control by established regulators through the implementation of hierarchical controls.[36] Examples of this approach range from attempts by the Government of China to directly control access to content,[37] to the less direct but equally effective regulatory techniques of western governments.[38] The second mechanism is *freedom from speech*. This is control through technology empowering individuated social values.[39] This is a more subtle but devastatingly effective methodology of controlling speech. Although internetworking technologies facilitate self-publication much more efficiently than previous technological advancements, they also facilitate self-censorship in an equally efficient manner. Through the use of filtering technologies individuals may filter out any speech they see as undesirable or as Shapiro puts it, 'the power of total

34 The author accepts that even the charging of such a small fee may be seen as hindering access. The costs of accessing cyberspace are though considerably higher than this fee. Therefore it is submitted that anyone who may access cyberspace may gain unhindered access to domain names.

35 Mueller, op. cit., n. 9, pp. 250–3.

36 A. Shapiro, *The Control Revolution* (1999) 64–73.

37 Measures for Managing Internet Information Services, Fazhi Ribao (Legal Daily), issued by State Council Order No. 292; signed by Premier Zhu Rongji on 25 September 2000. See, further, A. Neumann, *The Great Firewall: A CPJ Briefing* (2001), available at: <http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html> (visited 5 February 2003).

38 See V. Mayer-Schönberger and T. Foster, 'A Regulatory Web: Free Speech and the Global Information Infrastructure' (1997) 3 *Michigan Telecommunications and Technology Law Rev.* 45, at 46. Available at: <http://www.mttlr.org/volthree/foster.html> (visited 5 February 2003).

39 Shapiro, op. cit., n. 36, pp. 124–32.

filtering means that [undesirable speech] may be excluded effortlessly.'[40] With regulators exercising strong, even expansive, content control in cyberspace, and with users actively seeking 'essential credibility'[41] in the information that they receive, it would appear that speech is no more free in cyberspace than in real-space.[42]

As with rights in property the right to free speech or freedom of expression[43] has been subjected to intense legal and philosophical scrutiny. These analyses may usually be categorized into one of two approaches. The first is the democratic approach.[44] This requires the acceptance of democratic principles as the proper system for the governance of the state. It presupposes the existence of the autonomous decision maker seen in the works of Hobbes, Kant, and Mill *and* that individuals perform their duties as self-governing citizens within a democratic state. Not surprisingly, the democratic approach has developed in liberal democracies and is most clearly set out in the works of American scholars, in particular Meiklejohn and Sunstein.[45] The second methodology is the moral approach based upon chapter two of Mill's *On Liberty*.[46] This approach also presupposes the existence of the autonomous decision maker, it does not though require the existence of democratic sovereignty and as such is commonly characterized as the natural approach.[47]

1. The democratic approach

The democratic approach is premised on the view that freedom of expression is a necessary component of a society based upon the belief that the population at large is sovereign. Freedom of expression forms part of the democratic process and fulfils two requirements: (i) providing the sovereign electorate with the information it needs to exercise its sovereign power, and

40 id., p. 126.
41 M. Castells, *The Internet Galaxy* (2001) 198.
42 Pressures of space mean that this paper focuses only on controlling speech. Although freedom from speech is a key regulator in cyberspace it is unaffected by the propertization of the DNS and is therefore not germane to the current analysis.
43 For the remainder of this paper the right in question will be referred to as the right to freedom of expression. This is because, as T. Scanlon reminds us in his paper, 'A Theory of Freedom of Expression' in *The Philosophy of Law*, ed. R. Dworkin (1977), freedom of expression protects not only speech but also 'displays of symbols, failure to display them, demonstrations, many musical performances and some bombings, assassinations and self-immolations' (p. 155).
44 The democratic approach is characterized by Scanlon (id., pp. 154–5) as the 'artificial approach', because it is derived from and dependent on one particular theory of government, which is not universally accepted.
45 C. Sunstein, *Democracy and the Problem of Free Speech* (1993); A. Meiklejohn, *Free Speech and Its Relation to Self-Government* (1948).
46 J.S. Mill, *On Liberty* (1859).
47 See, for example, Scanlon, op. cit., n. 43, p. 155.

(ii) making government officials and public servants accountable to the population at large.[48] The democratic approach tends to value particular types of expression over others. As the value of free expression in the democratic thesis is premised upon the provision of information to the electorate and the accountability of officials, non-political expression is devalued at the expense of political expression. The democratic principle cannot adequately explain the United States First Amendment protection given to pornographic materials,[49] nor why purely artistic expression should be protected. Further, based as it is upon principles of democracy, it cannot adequately explain the value of the free expression principle in other systems of governance such as monarchies, oligarchies or meritocracies. This renders the democratic approach of little value when examining free expression in cyberspace. Within cybercommunities and cyberspace in general, the application of democracy is rare. Most cybercommunities are oligarchies, or constitutional monarchies, while a few are meritocracies. Very rarely is democracy encountered in cyberspace. For this reason the democratic approach is rejected as incapable of providing a philosophical foundation for the following analysis of free expression in relation to the developing jurisprudence of cyberspace.

2. The morality approach

Mill's approach is based on the quest for truth and enlightenment. Mill saw the free and unfettered exchange of ideas between men as the driving force behind the intellectual development of society. Individuals should be allowed the freedom to develop as individuals through the exchange of ideas between those whose minds have developed to the point where they are capable of being improved by argument and discussion. In Millian free expression theory, the best ideas will emerge from a market in competitive thinking, in effect, one which has unfettered expression.[50] Although Millian free expression theory is not without its critics, it has stood up well to the critiques it has endured over the years and was declared by Scanlon to be 'the only plausible principle of freedom of expression I can think of which applies to expression in general and makes no appeal to special rights (for example, political rights) or to the value to be attached to expression in some particular domain.'[51]

48 F. Schauer, *Free Speech: A Philosophical Enquiry* (1982) 36.
49 *Miller* v. *California* 413 US 15 (1973).
50 Another analogy, drawn by Schauer (op. cit., n. 48, p. 16), is that of the cross-examination process in the adversarial system of justice. By subjecting the idea to the maximum scrutiny the truth should emerge.
51 Scanlon, op. cit., n. 43, p. 162.

3. Locating free expression in cyberspace

In applying Millian libertarian principles today,we must identify whether the Millian model requires to be modified to reflect developments in society. Modern free expression principles recognize there are occasions when it is in the interests of society as a whole that speech be restricted or even suppressed. Scanlon identifies six cases where the exercise of free expression may cause harm to others and should therefore be restricted in the interests of the wider society.[52] These may be defined as cases where the risk to society caused by free expression outweighs the risks of suppressing free expression. How as a society do we decide when such restrictions on free expression are justified? According to Millian principles, once a community has reached the position of being capable of improvement by free and equal discussion, that community must protect freedom of expression. However, according to communitarian principles,[53] autonomous members of the community may believe that the state has a distinctive right to command them within certain limits and may agree to allow the state to override their right to make independent consideration within these limits.[54] In this manner individuals may agree to restrictions being placed upon their individual freedom of expression to serve wider community interests. When an adequate number of individuals within a society agree to allow the state (or other authority) to command them on a certain issue, tolerance of a command restriction may emerge. If individuals do not accept this command, they will throw it off.[55]

The development within cyberspace of communities that are capable of improvement by free and equal discussion is beyond doubt.[56] According to

52 They are: where the expression may bring about injury or damage; an (expressive) assault; defamation; causing alarm; contribution to another's harmful act, and speech which increases the ability of citizens to harm one another (id., pp. 158–9).

53 The communitarian critique of liberalism developed in the 1980s as a response to Rawlsian liberalism. Communitarianism represents three distinct critiques of libertarianism: (i) liberalism's alleged indifference to conceptions of human flourishing, (ii) its supposed exclusion of the pursuit of higher goals from the domain of politics and (iii) inattention to the ways in which a well-ordered society and a good life depend upon the exercise of virtue, the responsibilities of citizenship, and participation in a common political life. See: D. Bell, *Communitarianism and Its Critics* (1997); S. Avineri and A. De-Shalit (eds.), *Communitarianism and Individualism* (1992).

54 This may be seen as a communitarian update of Fichte's free expression theory. See L. Armstrong Smith, 'Johann Gottlieb Fichte's Free Speech Theory' (2001) 4(3) *Am. Communications J.*, available at: <http://acjournal.org/holdings/vol4/iss3/articles/lsmith.htm> (visited 5 February 2003).

55 id.

56 M. Major, 'Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution' (2000) 78 *Washington University Law Q.* 59; N. Netanel, 'Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory' (2000) 88 *California Law Rev.* 395; L. Lessig, *Code and Other Laws of Cyberspace* (1999) at

Millian theory, freedom of expression must be protected within such cybercommunities and within the community of cyberspace itself. According to communitarian theory, such freedom of expression cannot be restricted unless and until an adequate number of individuals within those communities accept the command of an identifiable regulator (the concept of the state does not 'fit' in cyberspace). This is not occurring in cyberspace. Rather, key regulators within cyberspace have imported restrictions on freedom of expression from the real world which have no place in, and which have not been accepted by, cybercommunities.

REGULATING THE DOMAIN NAME SPACE

1. The regulatory function of ICANN

ICANN is a private, California-based, not-for-profit corporation whose role is to:

> promote the global public interest in the operational stability of the Internet by coordinating the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet; perform and oversee functions relating to the coordination of the Internet Protocol (IP) address space; perform and oversee functions relating to the coordination of the DNS, including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system; overseeing operation of the authoritative Internet DNS root server system; and engaging in any other related lawful activity in furtherance of these items.[57]

This role, containing as it does management functions, standard-setting, and the promulgation of policy, defines ICANN as a private regulatory authority.[58]

Private regulatory authorities may take many forms and their legitimacy is directly related to the form and function of the regulator.[59] Scott classifies

ch. 6; H. Perritt Jr., 'Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?' (1997) 12 *Berkeley Technology Law J.* 413. For a counter-view, see Castells, op. cit., n. 41, ch. 4.

57 Articles of Incorporation of Internet Corporation for Assigned Names and Numbers (as revised 21 November 1998) Art. 3, at <http://www.icann.org/general/articles.htm> (visited 5 February 2003).

58 The term 'private' is being used here to connote a body in private ownership. Two distinct definitions of a private regulator are commonly used in regulatory literature. One is based upon a functional distinction the other based upon simple ownership. See C. Scott, 'Private Regulation of the Public Sector: A Neglected Facet of Contemporary Governance' (2002) 29 *J. of Law and Society* 58–60. The latter definition is preferred as a functional distinction would obfuscate the following analysis of private ordering .

59 The term 'legitimacy' is particularly fraught when dealing with private regulators. Legitimacy may be seen from a subjective or narrow viewpoint or from a wider objectively based viewpoint. For example within the confines of the Japanese Mafia

private regulators as falling within one of three families based upon their mandate.[60] These are: (i) private bodies who have a 'clear and official mandate based in statute', typically these are organizations who carry out a public regulatory function under delegated powers such as the Royal Society for the Prevention of Cruelty to Animals (RSPCA) or the Consumers Association; (ii) contractual bodies: regulatory authorities with formalized powers derived from contractual agreements;[61] and (iii) bodies with no mandate: these include a loose amalgamation of pressure groups, special interest groups, and industry associations who draw their regulatory power from the use of a variety of tools such as litigation, the publication and dissemination of information, and direct action.[62] In contrast to Scott's taxonomy, Schwarcz categorizes private regulators from a rule-making perspective.[63] He suggests that private ordering can be viewed as part of a broad spectrum within which rule-making is classified by the amount of government regulation or participation involved. Within this spectrum he recognizes four key classifications: (i) where rules are originated and put into force by sovereign governments; (ii) where rules are originated by private actors and put into force by sovereign governments; (iii) where rules are originated and put into force by private actors pursuant to governmental delegation; and (iv) rules adopted by private actors without government sanction.[64] These models are not exclusive of one another and when taken together provide an excellent overview of the structures of private regulatory bodies.

An examination of ICANN's mandate places it in the second of Scott's families, and the third of Schwarcz's. ICANN's mandate is based upon a series of contractual relationships between the organization and the United States Department of Commerce, the University of Southern California and individual domain name registries or 'registrars'. The regulatory mandate of ICANN may be found in two key agreements between ICANN and the

or Yakuza the punishment/atonement known as Yubitsume, which requires the self-amputation of a finger is a legitimate regulatory tool. Within the wider viewpoint of society as a whole this lacks legitimacy. This paper uses the term to mean perceived as legitimate *by the public.*

60 The following is taken from Scott, op. cit., n. 58, pp. 61–9.

61 This family may be internally subdivided between those based upon collective relationships, such as the Advertising Standards Authority and individuated relationships such as accreditation bodies.

62 This final family includes organizations such as the Federation Against Software Theft (FAST) and the Internet Watch Foundation (IWF). FAST is an industry association which uses litigation and the dissemination of information to regulate software piracy. The IWF is an industry association supported by all major United Kingdom ISPs which uses the publication and dissemination of information to regulate indecent materials, in particular child pornography on the Internet.

63 S. Schwarcz, 'Private Ordering' *Social Science Research Network Electronic Library*, ID 298409. Available from: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=298409> (visited 5 February 2003).

64 id., p. 7.

Department of Commerce: (i) the Memorandum of Understanding (MoU) between ICANN and United States Department of Commerce[65] and (ii) the Contract between ICANN and the United States Government for Performance of the IANA Function.[66] These agreements give ICANN de facto control of the legacy root.[67] Within the legacy root the pre-eminent server is the 'A' root server found in Hendon, Virginia.[68] Management of the 'A' server is carried out by ICANN as part of the 'IANA function' ceded by the Department of Commerce to ICANN under the Contract for Performance of the IANA Function.[69] As ICANN controls any changes to the root, anyone wishing to have a domain name visible on the Internet must acquire it from an ICANN-approved domain name registry. This control over individual domain name registries allows ICANN to contractually require registries to meet certain service requirements. At the forefront of these is the requirement that all registrants submit to ICANN's UDRP.[70]

65 25 November 1998, available at <http://www.icann.org/general/icann-mou-25nov98.htm> (visited 5 February 2003). The MoU has to be annually renewed, and at date of writing, the current version (Amendment 5) agreed on 19 September 2002 will remain in force to 30 September 2003 unless revoked under section VII. See <http://www.icann.org/general/amend5–jpamou-19sep02.htm> (visited 5 February 2003).

66 1 October 2002, available at <http://www.ntia.doc.gov/ntiahome/domainname/iana/SB1335-01-W-0650-0003.htm> (visited 5 February 2003). The Internet Assigned Numbers Authority (IANA), under contract from the US government, oversaw the allocation of Internet Protocol (IP) addresses to Internet Service Providers (ISPs). The contract for performance of the IANA function passes to ICANN responsibility for the tasks formerly performed by IANA.

67 Root servers play a key role in Internet navigation. Almost every computer on the Internet gets its data from one of these root servers, or from a cached downstream copy of their data. This is the result of the widespread use of a system program called BIND (Berkeley Internet Name Domain). BIND comes pre-configured to get data from one of the thirteen legacy root name servers and few users or domain name service providers ever change the setting. In practice this means only domain names recorded in the legacy root may be accessed by the overwhelming majority of Internet users. Although in theory any Top Level Domain is possible and may be added to the network, the legacy root is though the only root to which *all* name requests are sent by domain name servers. Thus any domain not recognized within the legacy root remains invisible to the majority of surfers. These domains may be 'made visible' by pointing your domain name server to one of these alternate roots, though most ISPs do not do this. For more on alternate roots see E. Rony and P. Rony, *The Domain Name Handbook* (1998) 513–72.

68 Of the thirteen legacy root servers, ten are hosted in the United States, and one each in London, Stockholm and Keio. The 'A' server is co-owned by the United States National Science Federation and Network Solutions Inc., a private Virginia corporation, now a wholly owned subsidiary of Verisign Inc.

69 op. cit., n. 66.

70 The ICANN Uniform Domain Name Dispute Resolution Policy (UDRP) is discussed in greater depth below. The policy may be accessed at <http://www.icann.org/dndr/udrp/policy.htm> (visited 5 February 2003).

2. Regulation through the UDRP

With control of the DNS, one can effect the ultimate cyber-sanction of banishment. ICANN may at any time, following a complaint in accordance with its domain-name dispute-resolution policy, order the removal of a domain name from the legacy root network. As all Internet users rely upon domain names for navigation, and as domain name servers invariably rely upon the legacy root to overlay an IP address on a domain name, the removal of a name removes that content from the easily navigable section of the network. It is the most elegant and efficient method of controlling content within cyberspace. Through the UDRP, ICANN attempts to substitute uniform global rules for what was once a largely territorial system of rights and dispute resolution procedures. It is important to note that as we have seen these rules were defined and implemented not by governments, but by a private, commercial regulator.

The UDRP has three main objectives:

(i) to create global uniformity for the adjudication of domain name disputes;
(ii) to reduce the cost of resolving such disputes; and
(iii) because of the sensitivity of replacing national laws with global law, UDRP adjudication is to be restricted to the most egregious types of cybersquatting, leaving all other disputes to national courts.[71]

It is contented that the policy has only fulfilled the second of these objectives. Its greatest failure lies with the third objective. The dispute resolution providers appointed under the UDRP dealt with 2,458 claims in the first year of the policy. It seems inconceivable that near two and a half thousand claims involving over four thousand domain names could all be described as egregious, particularly when compared to the number of cases litigated in the same period.[72] Further, an analysis of the claims reveals that dispute resolution panellists, who in many cases are untrained in the art of adjudication, are having to deal with complex cases involving competing rights in commercially valuable properties without the benefit of a hearing, the opportunity to examine parties, or to call for further evidence to be led. This has led to panellists' making naïve, and occasionally clearly incorrect decisions.

71 M. Mueller, *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy*, available at <http://dcc.syr.edu/miscarticles/roughjustice.pdf> (visited 5 February 2003) 4.

72 Twenty-seven cases were filed under the US Anticybersquatting Consumer Protection Act 1999 in the same period (December 1999–December 2000). In United Kingdom courts just four similar cases were heard in this period: *French Connection Ltd* v. *Sutton* [2000] ETMR 341; *WH Smith Ltd* v. *Colman* [2001] FSR 9; *Computer Futures Recruitment Consultants Ltd* v. *Stylemode Data Ltd* 2000 WL 33281329, and *MBNA America Bank* v. *Freeman* [2001] EBLR 13.

3. Resolving rights-based conflicts

Conflicts between rights-holders occur in all spheres. In real-space we are adept at recognizing the nexus between rights and have developed a sophisticated jurisprudence to deal with conflicts of rights. Broadly there are two dominant adjudicatory models found in real space: the adversarial model and the inquisitorial model. Both processes have distinct advantages and disadvantages,[73] and both share a number of common themes. First, both systems utilize a sophisticated jurisprudence to assist in dealing with complex conflicting rights from a variety of sources including, but not limited to: codes and other primary sources of legislation, judicial precedent, jurisprudential works, and sophisticated rules of procedure. Secondly, both systems are constructed around the 'finding' of the truth by the presentation of evidence to the court.[74] Thirdly, both systems employ a professional judiciary, trained in the processes of adjudication and experienced in the art of adjudication.

The UDRP, by comparison, does not contain the sophisticated jurisprudential foundations necessary to deal with such complex rights-based disputes. As previously mentioned, the UDRP was designed to deal only with the 'most egregious types of cybersquatting',[75] leaving all other disputes to the national courts. As a result the UDRP Rules are streamlined to provide a speedy and cost-efficient service, with no frills. The UDRP procedure is a simple arbitration procedure with none of the built-in safeguards found in real-space adjudicatory models. It is not a truly adversarial system as it lacks the necessary fluidity of an adversarial system. The procedure only envisages, and allows, the presentation of static documentary evidence: there is no opportunity for parties to develop or refine their claim in light of further evidence adduced by the other party.[76]

73 Research carried out in the United States suggests the adversarial method may reduce the bias of the decision maker and may lead to parties with a weaker factual case to more fully represent themselves (see J. Thibaut and L. Walker, *Procedural Justice: A Psychological Analysis* (1975)). The obvious disadvantages are the escalating costs and delays which may be involved in allowing parties to be masters of their own instance. Inquisitorial systems control costs and delays but risk subjective bias.

74 As directed by the Judicial Officer in the inquisitorial procedure and as revealed by the process of examination and cross-examination in the adversarial procedure.

75 A fact reiterated by Dr. Vinton G. Cerf, Chairman of ICANN, in testimony given before the House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet (8 February 2001) where he said, ''One of the policies that was generated from the ICANN bottom-up process early on was the need for a simple procedure to resolve the clearest and most egregious violations on a global basis. The result, after considerable work in a variety of ICANN forums, is the UDRP''. Testimony available at <http://www.icann.org/correspondence/cerf-testimony-08feb01.htm> (visited 5 February 2003).

76 The procedure is set out in full in the Rules for Uniform Domain Name Dispute Resolution Policy (UDRP Rules) available at <http://www.icann.org/dndr/udrp/

Similarly the procedure is quite unlike that found in traditional inquisitorial systems. Evidence is gathered and presented by the parties, not as directed by the panellist. Panellists, who may under Rule 12 request further statements or documents from the parties, are actively discouraged from seeking evidence outwith the four corners of the presented documentary evidence. The procedure is therefore extremely inflexible and unsophisticated as is to be expected of a procedure developed with aims of expediency and cost-effectiveness. This inflexibility hamstrings panellists when dealing with cases which extend beyond the ordinary. These problems may, to some extent, be resolved by a vigorous application of the flexibilities built into the UDRP Rules.[77] Such an expansive interpretation and application of the rules requires, however, that panellists are aware of the shortcomings within the procedure, and are sufficiently experienced in recognizing when the application of more complex and time consuming procedures is to the advantage of all parties. This would require that panellists be trained or experienced in the art of adjudication. A survey of panellists employed by the two major UDRP providers[78] carried out in April 2002 reveals, though, that over 57 per cent of the major provider's panellists and almost half of all panellists employed by the two major service providers[79] are untrained and inexperienced in adjudication.[80] Equally disconcerting is the finding that although only 42.2 per cent of WIPO panellists[81] are trained or experienced in the art of adjudication, 50.2 per cent describe themselves as experts in intellectual property (IP) rights. There is a concern that panellists with a background of practice at the IP Bar may fail to adequately reconcile

uniform-rules.htm> (visited 5 February 2003). Under Rule 3 the Complainant submits a written complaint. Rule 5 allows the Respondent to make a written response within twenty days. Following this, under Rule 8 there should be no further communication between the parties and the Panel, except through an appointed case administrator.

77 In particular, Rule 12 (discussed), Rule 10 which allows the Panellist 'to ensure parties are treated with equality, and Rule 13 which allows for in-person hearings in 'an exceptional matter'.

78 The survey, reported in full in the appendix, recorded 396 panellists employed by the World Intellectual Property Organisation (WIPO) Arbitration and Mediation Centre and the National Arbitration Forum UDRP Panel. As at February 18 2002 these two providers dealt with over 93 per cent of UDRP disputes (WIPO 59.2 per cent; NAF 34.4 per cent). Source: UDRP*info.com*, an ongoing survey of the UDRP process carried out by Professor Michael Geist of the University of Ottawa.

79 Some 152 of WIPO's 263 panellists had no experience or training in adjudication (57.8 per cent). In total some 194 of 396 panellists had no such training (49 per cent). Full details may be found in the Appendix.

80 'Trained' in this context means trained by an approved arbitration body such as the International Arbitration Forum or American Arbitration Association. 'Experienced' means the panellist has acted on at least three occasions (not being UDRP disputes) as an independent arbiter.

81 WIPO are the largest dispute resolution provider. They account for nearly 60 per cent of all UDRP decisions. See Appendix for further details.

complex issues raised in cases involving conflicts between rights of free expression and rights in property, and may by 'habit of thought' give extensive protection to any holder of IP rights. In doing so, they are failing to take account of the different dynamic of cybercommunities as compared to real world communities. Cybercommunities, as a general rule, value free expression more highly than real-world communities and as almost no one in cyberspace has voluntarily accepted the rule of ICANN they have not, in communitarian theory, accepted the command of the regulator in restriction of their free expression rights.

RESOLVING DISPUTES: THE UDRP AND THE PANELS

An attempt to strike a fair balance between the competing interests of parties is made by the UDRP Policy. Claimants under the UDRP procedure invariably seek the protection of Paragraph 2 of the policy[82] and in doing so they overwhelmingly cite trademark rights as the basis of the claim.[83] The policy aims to balance such claims by protecting the right to free expression through a legitimate interest defence contained in Paragraph 4. This applies when the respondent can demonstrate '*a legitimate non-commercial or fair use of the domain name without intent for commercial gain, to misleadingly divert customers or to tarnish the trademark or service mark at issue.*'[84] The defence is, though, poorly drafted and fails to adequately counter the extensive rights given to claimants under Paragraph 2.

Under most domestic trademark laws a purely non-commercial use is an absolute defence against a claim of trademark infringement.[85] ICANN's legitimate interest defence, however, falls short of this. Having drafted the non-commercial use defence as applying to 'any legitimate noncommercial or fair use of the domain name, without intent for commercial gain', ICANN, at the eleventh hour, added the further clause 'to misleadingly divert consumers or to tarnish the trademark or service mark at issue.' This

82 The full text of Paragraph 2(b) reads 'By applying to register a domain name, or by asking us to renew or maintain a domain name registration you hereby represent and warrant to us that … (b) to your knowledge the registration of the domain name will not infringe upon or otherwise violate the rights of any third party … it is your responsibility to determine whether your domain name registration infringes or violates someone else's right.'

83 The UDRP procedure represents the implementation of chapter 3 of the final report of the WIPO Domain Name Process, *The Management of Internet Names and Addresses: Intellectual Property Issues*, published 30 April 1999, WIPO Publication No. 439. The stated aim of this was to resolve the problems caused by the 'existing mechanisms for resolving conflicts between trademark owners and domain name holders [which] are often viewed as expensive, cumbersome and ineffective.'

84 UDRP Policy, op. cit., n. 70, para. 4(c)(iii).

85 Section 10 of the UK Trade Marks Act 1994, for example, lists several grounds of infringement, all of which require to occur 'in the course of trade'.

importation of the tarnishment concept seems wholly inappropriate and it substantially undermines the fair-use defence. In particular, this language could be used to deny protection to legitimate criticism sites. A site designed to attack a company's employment practices or environmental record might be considered to have the requisite intent to tarnish a mark. The UDRP protection in this area clearly goes far beyond current United Kingdom law in protecting trademark holders.[86] When the policy was enacted observers charged that the natural effect of this language blunted free expression protection for non-commercial users. ICANN was sufficiently concerned about these charges to include in its *Second Staff Report* a footnote stating:

> one detail of the policy's language should be emphasised. Several commentators indicated that the concept of 'tarnishment' in paragraph 4(c)(iii) might be misunderstood by those not familiar with United States law or might otherwise be applied inappropriately to noncommercial uses of parody names and the like. Staff is not convinced this is the case, but in any event wishes to point out that 'tarnishment' in paragraph 4(c)(iii) is limited to acts done with intent to commercially gain. Staff intends to take steps to publicize this point.[87]

In the three years following the statement, the only visible publicity, however, has been the posting of the report to ICANN's website. Crucially, ICANN appear not to have drawn the statement to the attention of the dispute resolution providers. This failure has led to a significant number of UDRP decisions finding non-commercial gripe or 'sucks'[88] sites to be in violation of the policy. Some of these decisions are highlighted in the next section.

1. Adjudicating complex cases

A survey, by the author, of thirty gripe-site cases decided before 8 February 2002 reveals that of thirty-one panellists involved in these complex cases involving conflicts between the free expression rights of individuals and the proprietary interests of trademark holders, only sixteen (51.6 per cent) were trained or experienced in the art of adjudication.[89] Further, the survey reveals

86 For further analysis of the concert of tarnishment of trademarks see M. Strasser, 'The Rational Basis of Trademark Protection Revisited: Putting the Dilution Doctrine into Context' (2000) 10 *Fordham Intellectual Property, Media and Entertainment Law J.* 375.

87 ICANN, *Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy* (1999) at <http://www.icann.org/udrp/udrp-second-staff-report-24oct99.htm> (visited 5 February 2003).

88 A 'gripe site' is a web site established to criticize an institution such as a corporation, union, government body, or political figure. They are also known as 'sucks' sites due to a common methodology of naming them NAME*sucks.com*

89 As 51 per cent of all panellists employed by the two major service providers are so trained or experienced, this indicates that there is no bias towards the selection of experienced panellists by parties when faced with such a complex case.

Table 1: Free expression decisions under the UDRP

Case No.	Provider	Domain Name Disputed	Outcome	Panellist	Experienced
FA0094964	NAF	Quirkmotors.com	Dismissed	Crary	Yes
FA0094959	NAF	Quirknissan.com	Name Transfer	Yachnin	Yes
D2000-0020	WIPO	Saint-Globain.net	Name Transfer	Glas	No
D2000-0868	WIPO	Skipkendell.com	Dismissed	Partridge	No
				Lockhart	No
				Mueller	No
D2000-0071	WIPO	CSA-Canada.com	Name Transfer	Ryan	No
				Fashler	No
				Sbarbaro	No
FA0094306	NAF	Lobofootball.com	Name Transfer	Carmody	Yes
D2000-0190	WIPO	Bridgestone-Firestone.net	Dismissed	Haviland	Yes
D2000-1455	WIPO	Mclanenortheast.com	Dismissed	Thomson	Yes
D2000-0584	WIPO	Dixonssucks.com	Name Transfer	Cornish	No
D2000-0996	WIPO	Guinessreallysucks.com	Name Transfer	Bridgeman	Yes
D2000-1015	WIPO	Lockheedsucks.com	Dismissed	Foster	Yes
				Sorkin	Yes
				Wagoner	Yes
D2000-0662	WIPO	Wal-martsucks.com	Name Transfer	Bernstein	Yes
D2000-0477	WIPO	Walmartcanadasucks.com	Name Transfer	Abbott	No
D2001-0843	WIPO	Dixons-online.org	Name Transfer	Carson	No
FA0097077	NAF	Michealbloomburgsucks.com	Dismissed	Sorkin	Yes

Table 1: (continued)

Case No.	Provider	Domain Name Disputed	Outcome	Panellist	Experienced
D2001-0007	WIPO	Accorsucks.com	Name Transfer	Le Stanc	No
FA00102247	NAF	Kendallhuntsucks.com	Name Transfer	Wallace	Yes
				Johnson	No
				Carmody	Yes
D2001-0376	WIPO	Cogema.org	Name Transfer	Willoughby	No
FA0097750	NAF	Misscleosucks.com	Name Transfer	Upchurch	Yes
D2000-0636	WIPO	Natwestsucks.com	Name Transfer	Cornish	No
D2001-1195	WIPO	Philipssucks.com	Name Transfer	Turner	Yes
D2001-0463	WIPO	Salvationarmysucks.com	Name Transfer	Gaum	No
D2001-0213	WIPO	ADTsucks.com	Name Transfer	Barker	Yes
				Wagoner	Yes
				Foster	Yes
D2000-0681	WIPO	Standardcharteredsucks.com	Name Transfer	Cornish	No
D2000-1406	WIPO	Dixons-online.com	Name Transfer	Ricketson	No
D2000-1104	WIPO	Wallmartcanadasucks.com	Dismissed	Perritt Jr.	Yes
D2000-0583	WIPO	Directlinesucks.com	Name Transfer	Cornish	No
D2001-1121	WIPO	Vivendiuniversalsucks.com	Name Transfer	Sorkin	Yes
D2001-0593	WIPO	Reg-Vardy.com	Name Transfer	Thorne	Yes
D2000-0585	WIPO	Freeservesucks.com	Name Transfer	Cornish	No

the rather surprising statistic that a transfer of the disputed name was ordered in twenty-three of the thirty cases (see Table 1). Of these, only eight cases were ones where the respondents were clearly acting in bad faith.[90] This means that of twenty-two cases involving complex rights-based disputes, the complainant was successful in fifteen: a success rate for complainants of 68.2 per cent. This rate of success significantly is higher than the success rate of complainants in all contested actions.[91]

In analysing some of the decisions, the risks involved in using an unsophisticated procedure to deal with complex rights-based disputes is clearly indicated. For example, the *Saint-Globain* case involved the use by shareholders of the company name as the basis for a domain name attached to a website critical of the management of the company.[92] The panellist, M. Glas, recognized their right to free expression but said the shareholders should have used a non-identical name.[93] This is a flawed decision. The policy does not distinguish between the use of identical or similar names when applying the legitimate interest defence.[94] This judgment clearly narrows the application of the legitimate interest defence. In doing so it prioritizes the emergent property interests of the complainant over the free expression rights of the respondents: the subtle balance the policy attempts to strike is lost. A similar misapplication of the UDRP is apparent from the case of *Dixons-Online.com*.[95] In this case an individual, Mr. Abu Abdullaah, used

90 These cases are: Freeservesucks.com, Dixonssucks.com, Guinessreallysucks.com, Natwestsucks.com, ADTsucks.com, Standardcharteredsucks.com, Philipssucks.com and Directlinesucks.com. In these cases cybersquatters had 'warehoused' several names involving well known companies and a sucks suffix. This had clearly been done with a view to profit.

91 Of the twenty-two complex cases surveyed, eighteen were defended actions. As at 8 February 2002, 1,254 non-default decisions were in favour of the complainant from a total of 1955, a success rate of 64.1 per cent. Data from UDRP*info.com* op. cit., n. 78.

92 *Compagnie de Saint Gobain* v. *Com-Union Corp*, WIPO D2000–0020, 14 March 2000.

93 'It goes without saying that shareholders or other interested parties have the right to voice opinions, concerns and criticism with respect to a listed company and that the Internet constitutes an ideal vehicle for such activities. The issue at hand is however not as Respondent seems to contend, the freedom of speech and expression but the mere choice of the domain name used to exercise this inalienable freedom of speech and expression. When registering the Domain Name, Respondent knowingly chose a name which is identical and limited to the trademark of Complainant and which is identical to the domain name registered by Complainant in the .com gTLD. [The] Respondent could have chosen a domain name adequately reflecting both the object and independent nature of its site, as evidenced today in thousands of domain names. By failing to do so, and by knowingly choosing a domain name which solely consists of Complainant's trademark, Respondent has intentionally created a situation which is at odds with the legal rights and obligations of the parties' Decision of M. Glas at Para. 6(c).

94 UDRP Policy, op. cit., n. 70, para. 4(c).

95 *Dixons Group plc* v. *Mr. Abu Abdullaah*, WIPO D2000-1406, 18 January 2001.

the Dixons-online.com domain name to run a consumer complaints service for which no charge was made. The panellist found that 'there was no evidence to conclude the Respondent is offering services or goods for any kind of commercial gain'.[96] Despite this they still found Mr. Abdullaah's use of the domain name to be illegitimate as:

> he is using the domain name primarily for the purpose of disrupting the business of a competitor. While it may be that the Respondent is not using its domain name for commercial gain, it has been held in several panel decisions that 'competitor' has a wider meaning and is not confined to those who are selling or providing competing products. In this wider context it means, 'one who acts in opposition to another and the context does not demand any restricted meaning such as commercial or business competitor'. In the present case, the Respondent is competing with the Complainant for the attention of Internet users which it hopes to attract to its site. Given also its purpose of acting as a complaint site, this seems evidence of both the Respondent's intention to acquire and use the disputed domain name in bad faith. While the interests of free speech and consumer protection may be advanced to justify the Respondent's acquisition and use of the disputed domain name, this is a .com domain name and clearly has the potential to disrupt the complainants business.[97]

This decision is in direct opposition to the spirit, if not the wording, of the *Second ICANN Staff Report*,[98] and presents such an expansive definition of competitor and competition as to be almost impossible to operate a gripe or complaints site within the scope of the defence offered by Paragraph 4. If this were a unique or even unusual decision it could be accepted as simply a 'bad' decision. Such decisions are though not uncommon. Within the list of cases on Table 1, similar unjustified restrictions of the legitimate interest defence may be found in several cases including, *Quirknissan.com*[99] *Lobofootball.com*[100] and *Csa-Canada.com*[101] Most tellingly perhaps, in the case of *Cogema.org*[102] a defence put forward by Greenpeace that, 'the use to which [they] intended to put the domain name was protected speech or expression under The European Convention on Human Rights and Fundamental Freedoms, Article 10' was rejected by the panellist as: 'The exercise of protected speech or expression under Article 10 of the European Convention on Human Rights and Fundamental Freedoms is … possible without confiscating the property of someone else.' These cases indicate that

96 id., para. 6.3.
97 id.
98 op. cit., n. 87.
99 *Quirk Nissan Inc.* v. *Michael J. Maccini*, NAF FA0094959, 29 June 2000.
100 *The Regents of the University of New Mexico* v. *American Information Services*, NAF FA0094306, 26 April 2000.
101 *CSA International (a.k.a. Canadian Standards Association)* v. *John O. Shannon and Care Tech Industries, Inc.*, WIPO D2000-0071, 24 March 2000.
102 *Compagnie Generale des Matieres Nucleaires* v. *Greenpeace International*, WIPO D2001-0376, 14 May 2001.

when faced with complex cases involving fundamental conflicts of rights, panellists all too often take the simplest way out which is to prioritize narrow proprietary rights over the free expression interests of the community at large.

As I have argued, however, according to communitarian theory, free expression should be protected within cyberspace unless and until an adequate number of individuals within cybercommunities accept the command of an identifiable regulator, in this case ICANN.[103] Clearly this has not occurred. ICANN's only source of regulatory authority is its contractual relationships with the United States Department of Commerce, and as the United States government receives no mandate from individual members of the cybercommunity, ICANN has no legitimacy to command individuals within these communities. The default position ICANN is required to adopt, according to communitarian principles, is to protect free expression interests over other interests until the legitimacy of ICANN to regulate expression is accepted by cybercommunities.[104]

CONCLUSION

The UDRP Policy lacks the sophisticated jurisprudential foundations required to adequately deal with complex rights-based disputes. This shortcoming is compounded by the lack of training given to panellists and the relative inexperience of panellists. It may be questioned why the loss of a domain name may be equated with suppression of expression. Many network commentators would argue that removal of a domain name following a UDRP decision does not suppress the free expression right of the losing party, as they may simply register a new, non-infringing, name and use this to resurrect the previous website with all content intact. They would argue that, as we have seen with the migration from Napster to AudioGalaxy and Gnutella, informational content will not be suppressed on the Internet. The current author respectfully disagrees. Decisions made under the UDRP do matter because in cyberspace the protocols are the key regulators of activity: ''*Code is Law*''.[105] Domain names play a key role as the addressing protocols of cyberspace: they uniquely act both as the naming and addressing protocol.[106] This means they both establish or designate identity and designate location. It is with respect to this second role as designator of location, that the censorial effect of UDRP Panel decisions becomes

103 See, above, n. 54 and related text.

104 Clear evidence that this has not yet been achieved may be seen in the large amount of anti-ICANN pressure groups. See, for example, <http://www.icannwatch.org>, <http://www.internetdemocracyproject.org/>, and <http://www.cpsr.org/internetdemocracy/>.

105 Lessig, op. cit., n. 56, p. 6.

106 See, above, n. 7 and related text.

apparent. Domain names are the road signs of cyberspace and the removal of these signs makes it significantly harder for individuals to find the information they seek: it is like trying to navigate the road network without any signposts. The content may still exist, but it may never be found.[107]

If there is even the risk of unjustified suppression of free speech through the application of the UDRP, it is essential that ICANN take steps to ensure that rights of free expression are fully protected. The Internet was founded upon libertarian values. Design protocols allowed for self-publication and anonymity; community values promoted free expression by combining public fora and the marketplace for ideas to create a 'new market for speech'.[108] The fabric of the Internet has changed with the commercialization of the network. Commercial actors seek to protect their 'property interests'. This includes the restriction of commercially damaging speech within the network infrastructure.[109] It is important that ICANN does not permit the UDRP to be used as a tool to suppress expression in this manner. An urgent review is needed, though not, as is often called for, of the UDRP policy itself,[110] but rather of the insufficiently sophisticated procedural rules employed by the dispute resolution providers.

107 Alternatively someone searching for such information may refer to a search engine. Here again though they may be thwarted. Businesses often 'buy' high ranking returns on common search terms such as their trading name, through advertising and other commercial routes. Although this is usually done for purely commercial reasons, a side-effect is that any potential ranking for a criticism site will be considerably lower in the returns generated, and is therefore less likely to be found.

108 See Shapiro, op. cit., n. 36, pp. 129–32.

109 This ranges from directly damaging speech such as copyright infringement, see *A & M Records Inc* v. *Napster Inc* 239 F 3d 1004 (2001), to simple 'gripe' sites, see *Lucent Technologies Inc* v. *Lucentsucks.com* 95 F Supp 2d 528 (2000).

110 M. Froomkin, 'ICANN's 'Uniform Dispute Resolution Policy' Causes and (Partial) Cures' (2002) 67 *Brooklyn Law Rev.* 605; M. Geist, 'Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP' (2002) 27 *Brooklyn J. of International Law* 903.

Methodology

As part of the current analysis it was necessary to carry out a biographical survey of UDRP panellists.

Sample Selection – Although there are four accredited UDRP service providers, two providers, the World Intellectual Property Organisation (WIPO) and the National Arbitration Forum (NAF) provide 93.66 per cent of all UDRP rulings (see Figure 1) and 88.69 per cent of all non-default (defended) UDRP rulings (see Figure 2).[111] A decision was taken therefore to focus the survey of UDRP panellists on those employed by these two providers.

Survey – Between 18–25 April 2002, the author carried out a survey of publicly available biographical data relating to all current WIPO and NAF panellists. These data were collected from on-line resources supplied by both providers.[112] The age and gender of panellists, their job or profession, the level of training and experience in relation to arbitration, and their nationality were recorded.

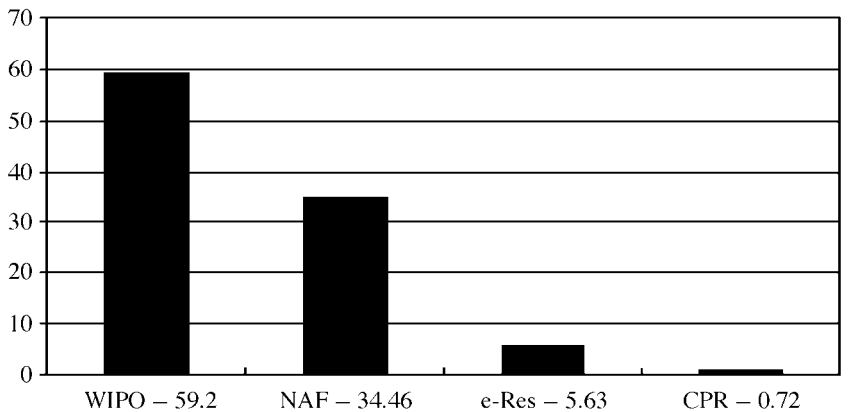

Figure 1 – Percentage Share of UDRP Market[113]

111 Figures correct to 18 February 2002.

112 WIPO details available at <http://arbiter.wipo.int/domains/panel/panelists.html>, NAF details available at <http://www.arbforum.com/domains/panelists.asp>. (Both visited 25 April 2002.)

113 Data in relation to market share were collected from UDRP*info.com* op. cit., n. 78. The data used was gathered on 18 February 2002.

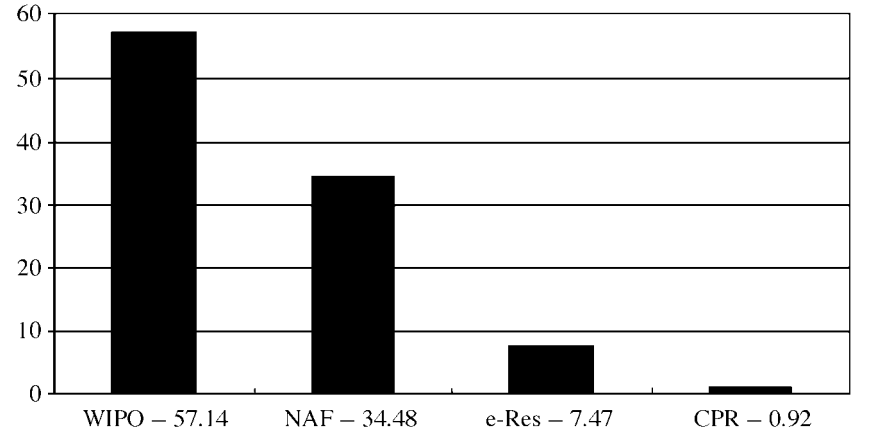

Figure 2 – Percentage Share of Non-default Decisions

Findings

The sample size was 396. This consisted of 263 WIPO panellists and 133 NAF panellists. Overwhelmingly panellists were male,[114] and were members of the legal profession (see figure 3). There was a clear distinction between the professional background of WIPO panellists, who were overwhelmingly practicing lawyers, and NAF panellists, a large proportion of whom were retired judges (see figures 4 and 5).

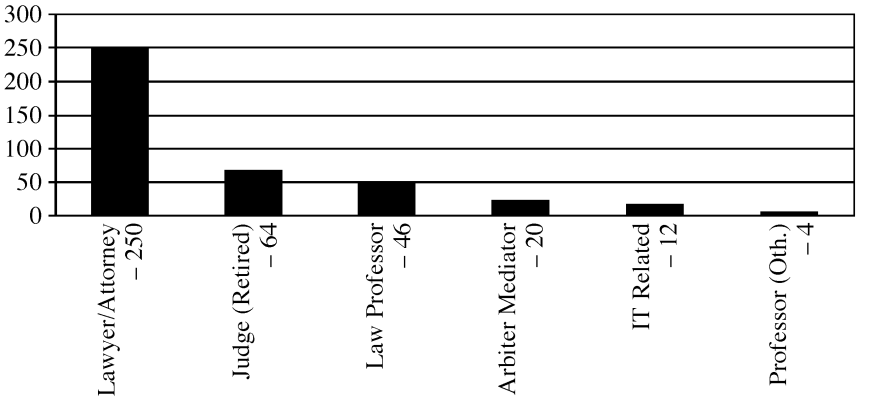

Figure 3 – Panellists' Professional Background (All)

114 Of 263 WIPO panellists only thirty-two (12.2 per cent) were female. The NAF biographical data unfortunately does not record gender of panellists.

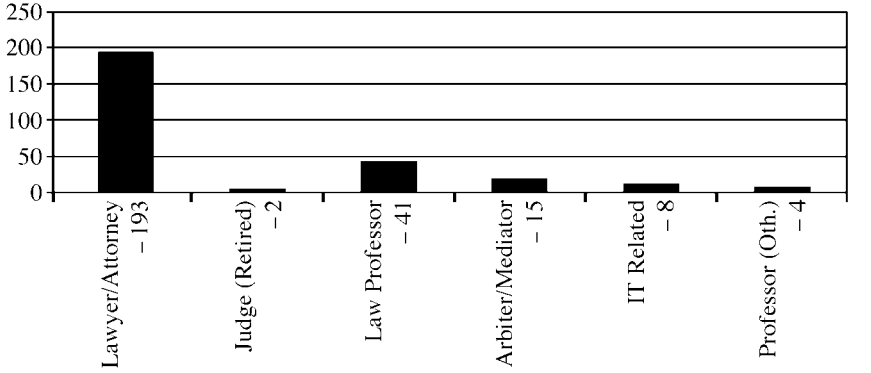

Figure 4 – Panellists' Professional Background (WIPO)

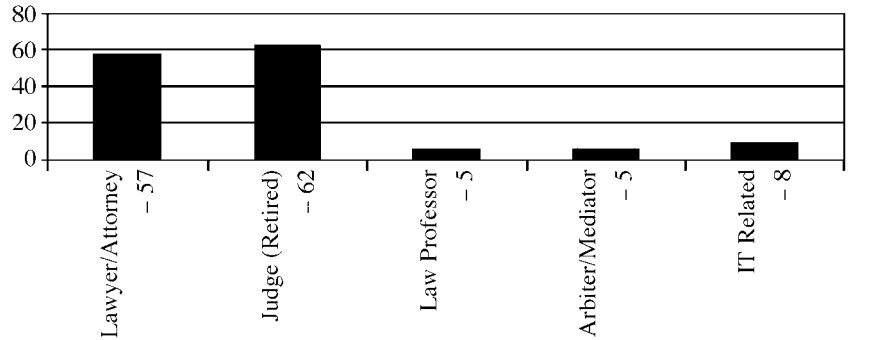

Figure 5 – Panellists' Professional Background (NAF)

Given the large divergence in professional backgrounds of panellists from the two major UDRP providers it is not surprising to find that there was a marked difference between the two in the proportion of their panellists trained or experienced in the art of adjudication.[115] As can be seen in Table 2, whereas 51 per cent of all panellists within the survey were trained or experienced in adjudication, only 42.2 per cent of WIPO panellists met this standard, compared with 68.4 per cent of NAF panellists. All WIPO panellists are offered the opportunity of attending training sessions on the UDRP procedure. Those who recorded this as their only training in arbitration are included in the third column. For the purposes of this survey, this does not qualify a panellist as being trained in the art of adjudication.

115 'Trained' in this context means trained by an approved arbitration body such as the International Arbitration Forum or American Arbitration Association. 'Experienced' means the panellist has acted on at least three occasions (not being UDRP disputes) as an independent arbiter.

Table 2 – Adjudicatory Training and Experience of Panellists

	Trained and/ or experienced	Not Trained	WIPO training only
All	202 (51%)	179 (45.2%)	15 (3.8%)
WIPO	111 (42.2%)	137 (52.1%)	15 (5.7 %)
NAF	91 (68.4%)	42 (31.6%)	0 (0.0%)

Given the greater experience in adjudication possessed by NAF panellists it raises the question of why WIPO remains the market leader in the provision of UDRP services. There are two possible reasons: (i) a preference for local panellists (geographical factor) or (ii) forum shopping and capture of panellists.

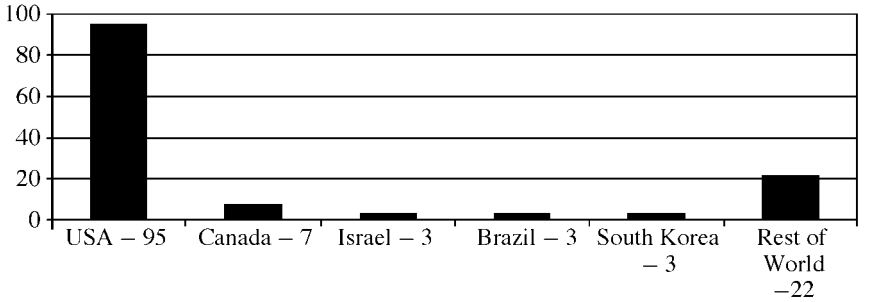

Figure 6 – Nationalities of Panellists (NAF)

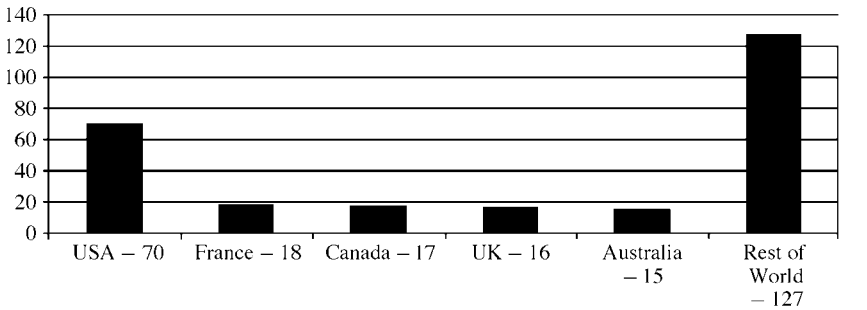

Figure 7 – Nationalities of Panellists (WIPO)

NAF is a United-States-based institution and appears to have a more US-centric approach. This can be see by comparing the nationality of panellists in both organizations. As can be seen from Figures 6 and 7, WIPO is clearly the more international of the two organizations. Whereas US-based panellists make up 71 per cent of the NAF panel, they make up only 26.6 per cent of the WIPO panel. This national bias is reflected in the complainant's country of origin. An

earlier survey by Milton Mueller[116] found that 92 per cent of NAF complainants were US-based, compared to only 60 per cent of WIPO complainants.

Despite the appearance of national bias, WIPO still attracts a proportionately higher amount of disputes than may be explained by the national origin of panellists. For example, 42 per cent of US-based complainants choose WIPO. This suggests the possibility of forum shopping and capture of panellists. Several studies have found evidence of forum shopping,[117] but these studies do not analyse the risk of capture. There is however, evidence that the WIPO procedure, in particular, is open to capture by trademark holders. WIPO is an organization 'dedicated to promoting the use and protection of intellectual property.'[118] It is not surprising, therefore, to find that the WIPO UDRP panel contains a high proportion of intellectual property practitioners. Of the 193 WIPO panellists currently practicing within the legal profession, 110 (57 per cent) list a specialism in intellectual property. In addition, of the forty-one academic lawyers listed, twenty-two (53.7 per cent) are listed as intellectual property professors or lecturers. Although it is to be expected that a high proportion of UDRP panellists would be experienced in intellectual property law given the nature of the disputes in question, and although there is no claim here made of individual bias by panellists in favour of intellectual property rights holders, for those panellists involved in the practice of IP law it may be difficult to maintain neutrality as the major aspect of their full-time vocation is the protection of IP rights from erosion and this might be expected to mean that certain 'habits of thought' are prevalent.

116 Mueller, op. cit., n. 71.

117 id., part V; Geist, op. cit., n. 110; M. Geist, *Fundamentally Fair.com? An Update on Bias Allegations and the ICANN UDRP*, available at <http://aix1.uottawa.ca/~geist/fairupdate.pdf> (visited 5 February 2003).

118 Taken from 'About Wipo' at <http://www.wipo.org> (visited 5 February 2003).