BILETA
British & Irish Law, Education and Technology Association
2007 Annual Conference
Hertfordshire 16-17 April
UH

Managing Virtual Communities: Time to Turn to the Whetstone?

Dr Martina Gillen
Senior Lecturer, Oxford Brookes University
Email: mgillen@brookes.ac.uk

What is a Virtual Community?

One-to-one telecommunications and relatively inexpensive air travel have not created any real communities. A sustainable community requires continuity, and the sharing of public conversation space. These characteristics are precisely what networked and computer-mediated communications are capable of, and the Internet[1] cybercommunities are a manifestation of this potential. These virtual communities are:

> "… social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace."[2]

The potential of cyberspace is not *simply* the creation of yet more "chattering" space. It has the potential of creating a virtual "public sphere" of the type necessary for healthy democratic governance in a well formed civil society. One important element of electronic communities is that they can help build up the weakening public sphere at a time when so many real world communities make individuals feel isolated and the public sphere is fading. Although there are problems in complete faith in electronic democracy, the hope is that:

> "… [the] technical trends in [Internet] communications technologies can help citizens break the monopoly on their attention that has been enjoyed by the powers behind the broadcast paradigm – the owners of television networks, newspaper syndicates, and publishing conglomerates."[3]

The Internet today has cybercommunities for everything – fantasy communities, ethnic communities, topical discussion communities, professional groups, game playing communities, etc. Two prominent categories of cybercommunities are Usenet and MUDs, or Multi-User Dungeons (Domains). In recent years a third category has been added those where the users create the content but the formation of the community is not user driven – for example the various blogging and picture sharing communities which can be described as "synthetic" as opposed to grassroots communities.

The most prominent collection of cybercommunities on the Internet is called Usenet. Usenet is a hierarchy of conversation areas called "newsgroups." In each of these newsgroups, users discuss topics by sending a message to the group and reading responses. In many of these newsgroups there is sufficient continuity and cohesion that each can be considered a genuine and stable cybercommunity.

Another set of communities is the Multi-User Dungeons (MUDs) and their more advanced versions MUD-Object-Oriented (MOOs). These offer a similar experience to the early textual computer adventure games where the user can undertake actions (including communication) by issuing commands such as "eat the cookie", or "say to Bill, 'Hullo, how are you?'" and receive responses. The

[1] Functionally, the Internet is an international network of computer networks - a network of networks - that allows the transmission of digital information among them. Various software applications around which communities have coalesced (including "Usenet", and "MUDs") have been built employing this functionality.
[2] Rheingold, H., *The Virtual Community*, Minerva, London, 1994, p. 5
[3] ibid., p. 289

immediacy of the interactivity on MUDs accelerates their development, and certain MUDs have attained a highly advanced state of community involvement. "Chat-rooms" are in many ways a subspecies of MUD, they allow direct communication but not all of them permit the performance of "virtual" actions. Many of them particularly those mediated by the Internet Relay Chat (IRC) protocol have long-standing networks and rooms with their own rules and approved behaviours.[4]"

The new "synthetic" communities where users create the content but do not "own" or cause the community to be created are generally generated by corporations and are characterised by an interest in a formal legal regulation which is not in keeping the traditional ethos of previous cybercommunities. This group of communities is becoming increasingly pervasive and this may well reflect a change and diversification in the users who wish to have a web presence. However, these services tend to be invitations to publish material and view the material of others. Even when an ability to link with others work or comment upon it is offered the spaces remain discrete and might not necessarily lead to community formation. The central argument of this paper is the consideration that whilst this third model will undoubtedly grow and perhaps eventually dominate the sphere it is not the only or necessarily the most effective means of community regulation.

The Paper Model

For the purpose of this paper the most interesting feature of this model is that the gatekeeper to control access to the community normally comes in the form of a user registration or user agreement document.[5] The key concerns of this kind of document are compliance with law and the avoidance of liability. Whilst this is appropriate to ensure that the companies concerned prosper and continue to be able to provide bandwidth and infrastructure. However, this broad contractual model, which is required to surmount the jurisdictional issues inherent in having global services, increases the complexity of the material that the user must deal with (if they ever actually engage with it at all[6]) and often leaves them with the feeling that the enforcement/protection mechanisms are remote.

Furthermore, in terms of micro-level community formation it has a number of difficulties. The emphasis on liability avoidance and adhering to legal norms has some overlap with the kind of characteristics that make for a strong community, however it does not on its own foster those behaviours. Thus, although the supply of infrastructure allows these companies to set the community rules they are qualitatively different form the old style "Stone" systems where the infrastructure providers remain intimately connected with the community as its core members. Essentially, this mode of regulation is not fit for this second task of actual community building because it is designed to match the needs of infrastructure creators for whom community is merely the secondary product of their enterprise.

The Stone Model of Regulation

In the more traditional cybercommunities the ultimate source of control differs between cybercommunities depending on how power is distributed within them. Whereas the technical power in USENET for example is well distributed, the power structure in MUDs like LambdaMOO is strictly hierarchical. The well known LambdaMOO virtual-rape saga concluded with the controller of the LambdaMOO environment, effectively the Xerox researcher who set up LambdaMOO, Pavel Curtis, managing a transition toward structures of democratic self-governance based on polling and elections.[7] Mr Curtis can orchestrate such a transition because he controls the computer programs underlying LambdaMOO, giving him ultimate control over the LambdaMOO environment. Given such omnipotent power, Mr Curtis's character within LambdaMOO - "Hakkon" - appears to other

[4] See Harris, D., *The IRC Survival Guide: Talk to the World with Internet Relay Chat*, Addison Wesley Publishing Company, London, 1995.
[5] See for example the LiveJournal agreement at http://www.livejournal.com/legal/tos.bml
[6] Although somewhat beyond the scope of this paper there is growing anecdotal evidence that many users have now simply become blind to EULAs and other click agreements and do not read them. http://www.techdirt.com/articles/20050223/1745244_F.shtml
[7] A document is available in the LambdaMOO virtual library called *"LambdaMOO takes a new direction"* which describes the transition http://www.cc.gatech.edu/classes/AY2001/cs6470_fall/LTAND.html

LambdaMOO denizens to be a "god", and the delegates of his supernatural powers are called "wizards".[8]

In LambdaMOO, the origin of all law *is* an omnipotent sovereign, the same sovereign that brought the community into existence by programming the virtual environment in which the community exists – Hakkon. Even the recent democratic reforms on LambdaMOO, which were intended to shift the role of governing the community from Hakkon to the characters themselves, does not sever the ultimate source of power – the "dominant will". The netizens of LambdaMOO themselves have commented in internal discussions that they should not fool themselves that they are truly masters of their own destiny.

The source of technological power is therefore either the creation of a new domain with its own rules, or superior knowledge of the rules of an existing universe. The examples above are "high-level" examples, i.e. they are closer to the informational "content" than to the electrons running down the wires. However, technical control over the "low-level" network protocols, which govern the transmission of information, may also be a source of power:

> "It is easy to overlook the fact that the message traffic over digital networks consists entirely of strings of binary digits. In this environment, the line between the meaning contained in message transmissions, and the purely technical contours of these messages, is blurred indeed …"[9]

Can these technical specifications then be seen as an integral part of the regulation of the Internet? I believe that they go beyond mere systems limitation, and even if they do not, it may be profitable to analyse them as such. The individual network protocols themselves possess certain inherent advantages in the competition for rule-making precedence in cyberspace, and this controller is therefore potentially the locus for much of the substantive rule-making that will take place there. To put it in other words, within a programmed environment a good place to begin a discussion of what the rules should be, is what is and is not allowed by the operating protocol. Many rules against spamming for example have this sort of basis: it is frowned upon not only as an irritating nuisance but also as a waste of the limited resources of the environment.
The "Stone" approach is based on control of the bedrock or founding resources and technologies of the Internet and because of that will always be an effective way of actually policing communities. On its own however, it can lead to autocratic and elitist communities which retrench the digital divide and ultimately fail to grow and develop. It is the argument of this paper that this model works best when married to the social concerns exhibited in the "Scissors" model.

The Scissors Approach

The evolution of community rules on the Internet is also dependent on the membership of the community and the communicative force of factions within fora such as the newsgroup "net.abuse" or the meetings within LambdaMOO. However, all rules require some sanction to secure enforcement so whilst the "Scissors" model can provide the values and direction for the development of community rules the sanction of social opprobrium must to be ultimately affective also be backed up by the technical mastery of the "Stone" approach that is why this paper proposes that the two should be used to enhance each other in the "Whetstone" model. In the physical world, the ultimate source of power, enabling such enforcement of rules, is physical power and the sovereignty of nation states. On the Internet, materiality and atoms have been replaced with signalling and electrons, wiring and cables. Cyberspace is a new universe where the laws of physics have been replaced with software and transmission protocols. Power is manifested by technically controlling or disrupting the communication of other users but in this approach the use of power is directed and perhaps constrained by the group opinion of the user community.

Thus, in addition to the technological power exercised by Hakkon and his wizards, LambdaMOO also has forums. Following the infamous virtual rape in that environment, intense discussion took place

---

[8] See Smith, J., *"FAQ: Basic information about MUDs and Mudding"* - available online at http://www.mudconnect.com/mudfaq/mudfaq-p1.html at paragraph 1.35

[9] Post, D.G., "Anarchy, State, and the Internet: An essay on Law-Making in Cyberspace", 1995 *J. Online L.* p. 3, paragraph 23

both at meetings in virtual rooms within LambdaMOO and newsgroups concerned with the activities in LambdaMOO. Julian Dibbel compiled some summaries of these discussions identifying the various factions within the LambdaMOO environment:

> "Parliamentarian legalist types argued that that unfortunately Bungle [the offender] could not be legitimately toaded [excluded] at all, since there were no explicit MOO rules against rape, or against just about anything else – and the sooner such rules were established, they added, and maybe even a full-blown judiciary system … the better …
>
> Others, with a royalist streak in them, seemed to feel that Mr Bungle's as-yet-unpunished outrage only proved this New Direction silliness had gone on long enough … high time the wizardocracy returned to the position of swift and effective leadership …
>
> For [the techno-libertarians] … assholes … [were] best dealt with not through repressive social disciplinary mechanisms but through the timely deployment of defensive software tools … Don't whine to the authorities about it – hit the 'gag' command …
>
> ...no position was trickier to maintain than that of the MOO's resident anarchists. Like the technolibbers, the anarchists didn't care much for punishments or policies, or power elites … complicated by the fact that the most vocal anarchists in the discussion [were] none other than legba … who wanted to see Mr Bungle toaded … Needless to say, a pro death penalty platform is not an especially comfortable one for an anarchist to sit on."[10]

That the attributes of the membership of these communities is determinative of the evolving set of rules, is also highlighted by feminist alarm at the lack of female presence on the Net. Dale Spender has written that:

> "At this very moment, as the road rules for the superhighway are being written and worked out, there is no critical mass of women involved to ensure that the highway code reflects some of their priorities and interests … "Netiquette" – as the new code is called – is another good example of the way men get there first and then stand guard at the gateway; their rules of entry are that you have to play their way if you want to be allowed on the road."[11]

The current set of rules on the USENET owes a lot to its computer science faculty origins and the prevalence of the libertarian hacker ethic. The cyberethic includes as its themes: a trust in technology coupled with a distrust of governments (techno-libertarianism), a faith in freedom of expression, and confrontational dialogue. On the Internet, everyone is playing a "game", where the players look to someone else to set the rules. Who is permitted to set these rules is a complex combination of technological control and influence gained via standing and status in the community which arises from long term commitment and contribution to the stability of the group in other words "social capital"[12] .

> "Social capital in the Internet is mainly expressed through what can be called *the community core*, which determines much of the sovereignty of the community in cyberspace. A community that has a united and engaged core of members may be able to confront threats more effectively and help regulators or play the role of regulators by controlling information and directing behaviour. The self-regulators need the discipline, compliance and support of members of the community to
> preserve the sovereignty of the community and therefore their power is not absolute."[13]

Thus, "elders" and "core" members of the community can constrain the actions of the "Wizards", direct the community generally as to the standards of behaviour expected and encourage self policing and community cohesion through norm setting and use of sanctions.

---

[10] Dibbell, J., "A Rape in Cyberspace - or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a society", *The Village Voice*, December 21, 1993, pp. 36-42. Also available at ftp://ftp.parc.xerox.com/pub/MOO/papers/Village/Voice.txt

[11] Spender, D., *Nattering on the Net - Women, power and Cyberspace*, Spinifex, Canada, 1995, p. 196

[12] Preece, J., *Online Communities: Designing Usability, Supporting Sociability*. Chichester, UK: John Wiley & Sons, 2000.

[13] Neumann, S., and Barzilai-Nahon, K., "Bounded in Cyberspace: An Empirical Model of Self-Regulation in Virtual Communities" Proceedings of the 38th Hawaii International Conference on System Sciences – 2005 at 5.

The most commonly deployed sanction is "flaming". A flame campaign occurs when many individuals across the Internet each post a vitriolic email or other message to the offender. Although the tone and content of these messages is usually enough to punish and deter the offender, the sheer quantity of messages can overwhelm the offender's email system and shut it down temporarily. Sometimes individuals will send a large message posted multiple times to achieve the same effect – a "mail bomb". The enforcers are, therefore, either outraged individual victims and/or volunteer vigilantes backed by a loose community consensus. In some senses, flaming is analogous to real world political protests or community based justice it is the community acting to police and control itself. The community can thus use social exclusion or public ridicule as a means of enforcing its mores without the assistance of the Wizards but without the ultimate threat of technological force there would be a proportion of offenders who could simply not be deterred. Hence the development of other sanctions which we shall now discuss which function successfully by blending the two approaches.

Cancelling others' messages is another means of enforcement. A user with a superior understanding of USENET software can enforce the rule against spamming by removing offending messages, through deployment of special software. For example, a prominent user (or group of users), operating under the pseudonym "Cancelmoose [tm]" has undertaken the role of enforcing the rule against spamming. "Cancelmoose [tm]" is able to cancel, despite objections by the authors of those messages, because of a superior understanding of USENET software. Spammers could, of course, if they were persistent enough, re-post their messages as soon as they were cancelled. Silencing can also be the result of the removal of historical records rather than contemporary postings.

Finally, we must consider the "capture" sanction. Capture is controlling another user's online character's actions or taking over their Networld identity. LambdaMOO is a fictional environment where characters controlled by users interact. Two characters on LambdaMOO were "virtually" raped. The "female" and "androgynous" victims were subjected to virtual violence and brutalisation seen by their corresponding users and the LambdaMOO community via text displayed on their screens.[14] The offender was able to coerce his victims' characters because of a powerful piece of programming called a "voodoo doll". This piece of programming allowed him to control the victim's actions by making it appear that his descriptions of their actions were originating from them. A third party with a more powerful piece of programming – a "gun" which "enveloped" him, eventually restrained the offender. Technology is the primary mode of control in cyberspace; however the most successful communities deploy technology in the service of group cohesion directed by those longstanding members of the community who have a stake in its future.

This kind of community management, combining the "Stone" and Scissors" models (what I call the "Whetstone" approach), ensures that communities remain strong and have a continuous ethos. Furthermore, these sorts of methods could also be used to enforce with the formal legal obligations of the "Paper" model to create self-policing communities which also avoided liability for the infrastructure providers. This kind of development however, would require some way of making sure that the content of the legal obligations became part of the value set of the community. It may be a beneficial strategy for corporations in this industry to have employees whose role is solely to be community members and elders and help build these ideas into communities rather than have them be ideas imposed from above which have little relevance in day to day community life. Companies might be wary of this as it could conversely also be argued that a more hands on approach could increase their liability by broadening their field of direct responsibility.[15] This perhaps is an area where some degree of rethinking of the legislative programme is required.

Conclusions

Cybercommunities are increasingly facing interference from physical communities. Electronic pornography, email harassment, defamation, etc., are arguably familiar activities in a new setting, which are increasingly attracting lawyers' and legislators' attention. Novel activities such as virtual-

[14] Dibbell, J., (1993, December 21). "A rape in cyberspace - or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society." *The Village Voice*, pp. 36-42. Available online at: http://www.ludd.luth.se/mud/aber/articles/village_voice.html

[15] By this I mean that there has been a certain degree of protection from liability extended to ISPs on that basis that they are a mere conduit of information (for example in the Electronic Commerce Directive) this would be lost if they began to take a more active role in selecting messages for transmission, deletion etc.,

rape, cancelling others' messages,[16] and spamming[17] are also attracting legal attention. Thus companies who are increasingly the providers of infrastructure and the starters of communities are focussing their gate-keeping activities on liability avoidance. This coupled with the weight of public opinion (which has become increasingly hysterical about the Internet) is a recipe for regulation.

However, examination of previous practice indicates that the creation of healthy communities is best facilitated by self-regulation by netizens and this may even assist in the attainment of some of the legally desirable behaviours as well.[18] An understanding of cybercommunities and their developing rules presents an alternative or addition to formal legal interference:

> "… [the Internet is] very antagonistic towards control, and making an effort to control it via the big stick is almost bound to fail, whereas educating, making people aware of the problem and making the community – because it is a community – aware that there are people who are misusing it and abusing it and offering them tools to help them change that is I think a far more productive way of going about it than simply attempting to legislate it out of existence.
>
> … remember there's something like 32 to 35 million Internet users out there who are using it … every day. They make a far more sensitive, and a far more effective screen than any single or even multiple law enforcement agency could ever form, and if they're educated, willing to assist and feel bound by a code of ethics to assist in stamping out material that they, the community, feel is inappropriate, they'll be far more effective than any law enforcement agency could ever hope to be. Neighbourhood Watch on the Internet!"[19]

The reputation of computer-mediated communication for being chaotic havens of deviance and rampant individualism is not entirely accurate. Cybercommunities are thriving, are important, and are currently dependent upon self-regulation for their survival. This regulation is not free from developmental difficulties or the challenge of external interference and internal conflict. However, bearing in mind the difficulties of regulating these cybercommunities by centralised authorities, potential community founders should attempt to understand and then consider internal governance as a regulatory tool. Internal governance has been shown to be an effective regulatory mechanism for even the most complex systems, the Panel on Take-overs and Mergers for example is still run upon a self-regulatory basis.[20]

Companies anxious to avoid liability have rushed to a legalistic model of regulation. They have done this without considering the history of this public sphere or its existing control mechanisms. It is perhaps time that they considered that the best way to make the Internet safe for their clients is not to regulate by contract alone but to empower, educate and motivate the users to regulate their space and respect the traditional user defined and oriented values and culture of the Web. Thus, Paper, Scissors and Stone working together could ensure that cybercommunities win.

---

[16] The legality of cancelling messages by 'Cancelmoose [tm]' was the subject of a very interesting discussion on the Cyberia-L listserv in late 1995.

[17] Himelstein, L., "Law and Order in Cyberspace" *Business Week* 4 December 1995

[18] Vadon, R., "Media Futures: Anarchists make the best police - Self Regulation is the way to stop offensive material travelling on the Internet", *Financial Times*, 29 May 1995, at 11

[19] Extracts from Transcript of panel discussion on ABC radio Australia (2CH) 13:05 18 April 1995. Comments are by Karl Auer. Quoted in Maltz, T., *Customary Law and Power in Internet Communities* available online at http://www.ascusc.org/jcmc/vol2/issue1/custom.html

[20] See the Panels homepage at http://www.thetakeoverpanel.org.uk/