Scan Journal vol 3 number 3 december 2006

Cyber Disobedience: Gandhian Cyberpunks

Cynthia Townley & Mitch Parsell

In response to those who have argued the Internet is amoral at best, and an instrument for immorality at worst, we show that the net can provide a forum for genuine ethical engagement and distinctive forms of wrongdoing. Without deriving the moral value of the Internet from its interface with the non-virtual world and in contrast to presentations of the net as an anarchic utopia or as an unethical or amoral dystopia, we apply a substantive moral test to a selection of online examples and ask can the net accommodate resistance to oppression that is necessary, though not sufficient, for justice? More precisely, we will ask whether Gandhian non-violent action is available to Cyberpunks?

We use the term Cyberpunk both more broadly and more narrowly than is standard.Cyberpunk proper is a sub-genre of science fiction focused on a liberal mix of high technology and marginalised characters; of advanced computer and information technologies existing in a future featuring significant social decay and civil breakdown. William Gibson's archetypal *Neuromancer* contains classic cyberpunk characters: "marginalized, alienated loners who lived on the edge of society" (Person 1998). For Gibson, a Cyberpunk works against traditional power structures. We co-opt this figure of a non-conformist using technology to contest, dissent from or combat a questionable status quo. Someone who hacks merely for personal gain is not a Cyberpunk on this definition – hence our use of the term is narrow than usual – whereas a contributor to the Wikipedia with little or no technical skill may well qualify – hence our use is wider than standard. Our Cyberpunks need not be loners. Just as Gibson's characters cooperate in various projects, so do our cyberpunks. And necessarily so – the net is always a collective endeavour, a project of interdependence. Interdependence and vulnerabilities are the ground for both ethical practices and injustice, communities are characterised by conflict as well as mutual support. It is the type of practice that characterises Cyberpunk, not the number of participants. Later, we distinguish those Wikipedia interventions and intervenors who add to the anarchic character of the net, from those who seek overall control.

Mahondas Gandhi (1869-1948) articulated a theory of non-violence and deployed it in political struggles in South Africa and India. Gandhi argues that conflict, including violence, is always a form of untruth. When I insist that my actions are justified but you see them as oppressive, there is a truth of the matter that at least one of us is failing to acknowledge: "The basic principle on which the practice of non-violence rests is that what holds good in respect of yourself holds good equally in respect of the whole universe. All mankind in essence are alike…" (Gandhi: 315). Gandhi's followers or *satyagrahi* hold to a truth that is emergent and provisional. Gandhian non-violence or *ahimsa* demands that its practitioners hold to the possibility of a shared truth, to the possibility that the other party is capable of recognising it, and that the ultimate recognition might not be that envisioned by either side initially. Hence, to coerce others' agreement would be self-defeating. We use Gandhi's non-violence as our moral litmus test. Non-violent resistance is directly relevant to the non-conformist nature that the net sometimes displays and that is thought by many to be one of its merits.

Between utopia and dystopia

Early net adopters were optimistic about the web's power for good. The world was going to change because the ability to exchange information quickly and efficiently with distant confederates would enable the disadvantaged and stereotyped to participate without prejudice. New and exponentially expanding information opportunities would generate solutions to many of the world's practical problems, traditional activities would become less wasteful (the notorious paperless office) but most importantly, technology would be the new force for equity.

Some radicals were particularly optimistic about the political implications of the Internet. These Cyberpunks saw the net's equalising potential as a real opportunity to decentralise control – control of economic resources, intelligence, political

power and the like. The net, they claimed, could have a profound and positive impact on the nature and structure of society. This movement hits its peak with Tim May's crypto-anarchism. According to May and his supporters broad Internet adoption together with the availability of encryption software would make an anarchist state inevitable. Indeed,

> These developments will alter completely the nature of government regulations, the ability to tax and control the economic interactions, the ability to keep secrets, and will even alter the nature of trust and reputation (May 1992).

In this brave new world, government control will be eroded, people will associate and transact freely. The freecycle network (www.freecycle.org) is just one example of an alternative to regular financial interaction.

Others saw the net as a trap for the unwary, ruled by vice, ignorance and deceit. When identities can be infinitely fluid, there is no accountability. Anyone can do anything, hide anything or propose anything.

Neither utopian nor dystopian predictions eventuated. Despite the cyber-punks' hopes the net has not produced anarchy. Business continues much as usual, but in ways that undermine the reactionaries' concerns (see Townley and Parsell 2004; de Laat 2005). Sites for commercial transactions such as e-bay use feedback to make others' assessment of reliability or trustworthiness transparent to all users, and various conventions and expectations for contributing to and comprehending the feedback systems have arisen. But more interestingly, the anarchists were right that the net would dramatically change the nature of government control and the net has increased the democratic nature of the media, leading to new models of communication and information, models approaching if not yet implementing anarchist ideals. The now familiar blogs and wikis, and integration of user-generated content into mainstream news media are perhaps the most vivid demonstrations of a radical democratisation of information dissemination. The reactionaries were correct, as 9-11 and later developments devastatingly documented, that the net could be used to coordinate monstrosity.

But in the face of the net's apparent development as (among other things) a set of flourishing communities, William Galston (1999) and Hubert Dreyfus (1999) have questioned the net's capacity to generate communities and meaningful interactions. Online interactions are too transitory and shallow to inform substantial norms and moral standards unique to the Internet so they conclude that Internet communities are miscalled, they are at best "sham" communities. It might seem obvious that as a playground for human interaction, the net is an environment for community. But this is precisely what Galston and Dreyfus deny. At best it is an imitation whose value is either illusory or derives from real world effects. Of course, the net is not hermetically sealed: the interactions on which an e-bay rating is based cross into the real world. Our point is not that the net can or should be understood in isolation, but that in coming to understand its intersections with the physical world, sufficient weight has to be given to the net on its own terms. Contrary to Dreyfus and Galston, Internet-based communities develop and implement their own norms and conventions. To avoid question begging, we take "community" very broadly such that any shared practice *can* count as forming a community. Galston's notion of community is much thicker. Following Thomas Bender (1982), he requires limited membership, affective norms, shared ties and mutual obligation. Galston's central point is that the flexibility of the online environment dissolves the mutual obligation required to support real community. When a community is threatened or takes a direction we find disagreeable, instead of working with our fellow members to strengthen or change the community, we simply leave or form a new group. Online practice, particularly attempts at in-group reform, appears to count against Galston's contention. Galston could object that such responses are superficial. This is one reason why applying the standard of Gandhian non-violent practice is important – the online activity needs to be morally robust in order to support revisionary activities. Our examples show within a relatively constrained community, with respect to massive common projects such as Wikipedia and in cyber protests, participants can and do operate online as community members in the most robust sense.

The text-based "community" of LambdaMOO undertook internal revisions in response to the now *in*famous case of cyber-rape. While not cyberpunk activity, this case exemplifies group-based reform rather than individual exit from a community. In 1993, a character named Mr Bungle enacted a violent sexual assault on two other characters, Starsinger and legba. (Obviously, cyber-space violence is simply not reducible to external harms, and a rape described in the interactive text of an

online community differs importantly from descriptions in traditional texts that report or imagine such an event. It is philosophically interesting, but not something we have the space to discuss, that the text both describes *and* performs the wrong). Redress for the crime was sought within the community and ultimately his punishment was banishment. Although almost universally acknowledged as a destructive and reprehensible crime within LambdaMOO, the Mr Bungle incident prompted reflection on the degree and type of regulation the community might require, and explicit consideration of and debate about the nature of the community itself. The community's members developed a dispute resolution and community petition process. These events demonstrate that norms of appropriate behaviour and sanctions for inappropriate behaviour can be developed internally to net-based communities. Of course, together with the many well-functioning, self-regulating communities online there are also many non-benign versions. Nevertheless, the image of the Internet as an environment of unconstrained fluidity, deceit and misrepresentation, incapable of eliciting shared ties and mutual obligation is excessively negative.

So far, we have countered the net pessimist's insistence that the very notion of virtual *communities* is problematic. Online interactions, they argue, lack the necessary resources to develop communities in the requisite robust sense. Internet groups are instantiated in virtual spaces that permit and value extraordinary personal freedom, fluidity and flexibility. And this is too impoverished a base for true community engagement. Both group mobility (Galston 1999) and the lack of a personal commitment (Dreyfus 1999) will make online groups especially susceptible to malicious individuals which will cause their permanent break-down. This reaction stems from the misconception that the structure of the net lacks incentives and even conditions for personal investment and reciprocal concern for personal damage. LambdaMOO's response to Mr Bungle indicates otherwise. When online groups are confronted with malicious behaviour they do not simply disband, but are prepared to invest resources into developing norms of behaviour and sanctions for breaking those norms. We now move to Gandhi's conception of non-violent action and its application in cyberspace.

Virtual Satyagraha

Gandhi and his followers advocate *satyagraha*—truth insistence or non-violent resistance—as the only ethical way to oppose injustice. Injustice is a failure to recognise in action or thought the fundamental truth of others' moral standing. Gandhi argues that it is only by bringing a perpetrator of injustice *face-to-face* with a morally grounded opposition that improvements in justice can be achieved. The truth is the only resource with the power to make injustice take flight – violent or coercive responses can only provide further reasons for retaliation, thus constituting and/or provoking further injustice. Gandhi's followers put their bodies on the line, and Gandhi does not flinch from the reality of sacrifice in the cause of truth and justice.

This model does not seem applicable to cyber-protest. Face-to-face interactions and their vulnerabilities are precisely what the Internet lacks. But insisting on the presence of a body guarantees that all human reality is embodied reality, and not virtual reality, and this debate should not be fought by definition. Nevertheless, there is at least a prima facie plausibility to the claim that cyber-encounters lack the direct manifestation of the reality of the human situation that is the ultimate grounds for truth insistence. But as the Mr Bungle case should already suggest, violence towards other moral agents can result from nothing more than words. And the manifestation of virtual violence might well be matched by virtual *ahimsa* or non-violence.

A reconsideration of Gandhian non-violence can make sense of this. Non-violence is not a mere refraining from overt physical assaults on others. Conversely, violent action is not always reducible to physical force. Threats may be "merely" verbal, torture "merely" psychological, and nevertheless such actions are coercive and violent. Gandhi's conception of *satyagraha* entails truth-insistence, acting in the face of others' oppressive and aggressive conduct in a way that opposes it not with counter attack, nor defensive preparation against attack, but steadfast insistence on the right that the other's violence or dogmatism is violating. So the salt marchers disobeyed the prohibition on their harvesting of salt, by calmly walking to the shores, and collecting the banned stuff.

By presenting resistance without violence, *satyagrahis* insist on the truth and justice of their claims. Thus it becomes

incumbent on those opposing them to identify what was wrong with this action, and to defend or renounce their own imposition of the salt ban or other controversial restriction. According to Gandhi, this is how truth insistence works. It makes manifest the reality of the situation, and rational agents, humans, then come to recognise what is going on. Nothing prevents cyber-action being understood along these lines. To the extent that cyber-disobedience is non-violent, and aims at redressing repressive power structures by demanding the defense or abandonment of those structures, it would qualify as legitimate and morally defensible on this dimension of the Gandhian model. But Gandhi demands more than non-violent and confronting behaviour. Not all non-violent protest is justified. Protestors must accept that they may also need to change their view. Indeed, a fundamental aspect of Gandhi's thick conception of non-violence is being prepared to accept truth from any sources. One must always be willing to change in the face of truth, in contrast to the dogmatic refusal of the possibility that someone else, even one's apparent oppressors, might have a legitimate point. Thus, Gandhi provides a thoroughly dynamic model of protest. Such an open, dynamic interplay must also be demanded of non-violent cyber-disobedience. Legitimate cyber-disobedience is a process of opposing injustices and aiming for openness, rather than aiming for some predetermined outcome worked out in advance by the Cyberpunk. In the remainder of this paper we will demonstrate the power of this mode of ethically evaluating online behaviour by examining three recent cyber incidents: (i) the proposed tightening of controls on the Wikipedia: (ii) Google's decision to provide an censored service in China; and (iii) the use of denial of service (DoS) -like attacks by the Recording Industry Association of America (RIAA). Our discussion offers grounds to take (i) to demonstrate that despite much Cyberpunk rhetoric to the contrary, increased control does not mean abandoning Cyberpunk ideals. In fact, we suggest that in the case of the Wikipedia increased control might not only strengthen that community, but be necessary for achieving Cyberpunk ends. Of course, increased control is not always a good thing. In some cases, the control of dissidence or deviance is worse than the "problem." We take the Chinese Government's attempt to control access to online information as a case of this type and examine Google's apparent acquiescence to this oppressive over-regulation. We take the issues raised by (ii) and a Cyberpunk response to be ethically complex and although we will not attempt to say whether Google are in the right here, we will demonstrate that our notion of virtual *satyagraha* has the necessary resources to provide the answer. Finally, we establish that although (iii) has many of the features commonly associated with Cyberpunk activities it is not morally defensible according the model we provide.

The Wiki Wars

Wikis allow anyone with a web-browser to create web content. Because no-one owns or controls the content of wiki pages, wikis are as close to large scale Internet anarchy as anything presently available. Indeed, such open editing in theory enables anyone to become a Cyberpunk by encouraging the composition of site content by non-technical and non-specialist users. The most widely known and ambitious wiki is the Wikipedia.

The Wikipedia (http://en.wikipedia.org) is an online encyclopaedia promoted as "the free encyclopedia that anyone can edit." This makes the Wikipedia significantly different from any traditional encyclopaedia that relies upon contributions from carefully selected experts. Wikipedia's publicity claims that its entries are open to correction by anyone, allowing broader and more inclusive content. This aspect of the Wikipedia has been widely celebrated. Time.com proclaimed it Internet-enabled egalitarianism (Anderson 2006). But all is not well with the Wikipedia and its democratic nature has turned out to be its fatal flaw.

Ironically, the representatives of democratically elected officials have done the most damage to the Wikipedia. Members of the US Federal government have been implicated in editing Wikipedia entries for political, not informational purposes. Aides to Massachusetts Democrat Marty Meehan deleted references to his broken term-limits pledge and massive campaign war chest (McCullagh 2006). Other edits played up the link between al Qaeda and Saddam Hussein. These abuses have led to proposed changes to the Wikipedia editorial policy: there are calls to require all editors to register. Some Wikipedia contributors have objected to this, seeing it as reactionary and a denial of anarchic openness. A closer examination of the Wikipedia reveals that it never was anarchic. More importantly, its effectiveness as an open information resource depends on an accountable community.

The Wikipedia has always implemented a very traditional editorial power structure: "a perfectly bureaucratic and

hierarchical means by which articles and editions are managed" (Racoma 2006). Indeed, the Wikipedia structure is a standard power pyramid:

> At the bottom are anonymous contributors, people who make a few edits and are identified only by their IP addresses. On the next level stand Wikipedia's myriad registered users around the globe ... the next level – administrator ... can delete articles, protect pages, and block IP addresses. Above this group are bureaucrats, who can crown administrators. The most privileged bureaucrats are stewards. And above stewards are developers, 57 superelites who can make direct changes to the Wikipedia software and database. There's also an arbitration committee that hears disputes and can ban bad users. (Pink 2005).

The proposal to demand registration removes the bottom-layer. It does not change the power structure or compromise its openness. Indeed, the proposal promises to strengthen the Wikipedia's openness by promoting the development of an accountable community.

Open edited resources are prone to abuse. Such abuse can be handled in two ways; externally by legal sanctions or the like being imposed, or internally by the development of norms by the resource's community of users. External sanctions are likely to lead to tighter restrictions on use and to close the open nature of the resource. But internally developed and implemented control need not compromise openness. The Mr Bungle case actually strengthened the LamdbaMOO community and led to renewed critical examination of its values and aims. Requiring registration to edit the Wikipedia may produce similar results. One problem with the Wikipedia is its failure to build a community because contributors are not required to defend their contributions. Without demanding such responsibility the Wikipedia fails to provide a forum whereby community building can take place. A second problem is a lack of transparency – the Wikipedia is not up front about its own editorial policies and power structures – indeed, its claim to anarchy is misleading at best. Both problems reveal a lack of mutual obligation, a key element Galston identifies. By requiring registration the Wikipedia could provide resources for the type of internal dynamic criticism that encourages reflection on and development of norms, standards and sanctions, and an environment in which accountability to the community is explicit and transparent. And demanding such registration is a bar to neither openness nor democracy. To demand strictly anonymous contributions to a resource aimed at the presentation of knowledge, is to misunderstand the value and nature of openness, democracy and knowledge. Anonymity from the community devoted to these ideals is in fact counter-productive. If it is guided by openness, democracy and knowledge, recognition by the community is not an evil to be avoided, but a virtue to be enjoyed. Of course, if a community is repressive, dictatorial or un-responsive to truth, anonymity can be of great value. Indeed, the building of or participation in communities that promote openness and truth is seen by some political regimes as subversive. Then anonymity should be respected. Dreyfus (1999) fails to see this benefit to anonymity, arguing that it is always a bar to the development of deep commitment to one's position. In our view, anonymity from repressive regimes is required to develop just the commitment that Dreyfus finds most meaningful in life: commitment to intellectual curiosity. We turn now to a case where anonymity seems clearly valuable.

The Google Dilemma

The Internet as a vast repository of information is a significant ally of those opposed to repression. Oppressive regimes concede its threat. The Chinese authorities, for example, censor the online information citizens can access. In a decision that shocked many, Google recently launched a Chinese search (google.cn) service that "that respects the content restrictions imposed by Chinese laws and regulations" (Wickre 2006).

Google have defended their Chinese service as a compromise that actually increases the information reliably deliverable to Chinese clients. The Chinese Government was filtering requests sent to the Google server and the results Google delivered to the user. Many politically sensitive search strings (e.g., "human rights" "political reform," "Tiananmen Square" and "Falun Gong") simply failed to reach Google. So rather then having their service externally censored, Google opted for self-censorship. Elliot Schrage, vice president for global communications and public affairs at Google, stated in his testimony to the US House of Representatives that "our decision was based on a judgment that Google.cn will make a meaningful –

though imperfect – contribution to the overall expansion of access to information in China" (Wickre 2006).

Not everyone is happy with the compromise. Amnesty International USA's Online Action Center responded by providing detailed instruction on using Google support systems to log complaints about Google compromising Chinese freedom. It is not our intention to side with either Google or Amnesty on this issue, but to examine the validity of Schrage's appeal to a meaningful contribution to increased information.

Google's move aims to produce greater openness, although, paradoxically this takes place via substantial constraints. Suppose the censored Google is the only online search engine available to Chinese net users. They have greater informational access with this service than without it. It is, however, also relevant to compare the Chinese users with all net users. Here, the relative disadvantage of those using the censored version shows up clearly. By acquiescing to unfair patterns of access, Google appears to have compromised a good offered by the Internet. However, some considerations tell against this initial reaction. First, when Google.cn delivers censored results this is clearly indicated to the user. Second, Google.cn is an addition to, not a replacement for Google.com. Thus the user is both informed of censorship and provided with another service that is not censored. But here the Chinese citizen would appear to confront the problem that was the catalyst for Google providing their special Chinese service: the direct censorship of the regular Google.com service by the Chinese Government. A Cyberpunk response offers a means to circumvent this control: anonymous browsing.

Anonymizer® Inc. launched Operation Anti-Censorship in March 2006 and created a service specifically for Chinese citizens which enables safe access to the entire Internet. This is achieved by circumventing the Web filters put in place by the Chinese authorities and further protects users by shielding their personal identities. Such a service evades the Chinese tracking system and enables any user to anonymously access pages and search engines without the risk of being identified as subversive. Searches are unrestricted and users are untraceable. This technology is an example of an anonymous proxy server. A good anonymiser will modify an accessed webpage so that all links in it point back through the same proxy. Thus from the outside it will appear that you are merely accessing the proxy, not the resources the proxy is itself delivering.

This technology is an imperfect solution. First, anonymisers slow access and thereby place Chinese users at a disadvantage. This is a minor problem, especially if the service is only used when censorship is an issue. Google's indication of censored results and continued operation of its full service enable this systematic use. Second, the technology is not perfectly benign, since it undermines legitimate forms of control and scrutiny of net usage. It not only enables Chinese political inquiry, but potentially advantages those looking for more dangerous information, for example about weapons or drug manufacture. Of course, parallel arguments have been used to censor books and other virtual sources of information. Thus, although opening a complex ethical domain, anonymisers do not in this respect produce any unique ethical dilemmas. Third, it is not clear that the use of an anonymous proxy will confront the Chinese authorities in a manner that demands dialogue and engenders the possibility of political change.

The Gandhian model of non-violent action requires confronting those identified as oppressors. Amnesty's response to Google achieves this by using online resources, and hence qualifies as a legitimate non-violent Cyberpunk protest activity. The use of anonymous proxy servers, however, lacks this confrontational aspect. The point of the proxy is that one's net interactions go untracked. Hence, such use is certainly not directly confrontational in the same way as Amnesty's response. Nevertheless, the Chinese authorities will be faced with what they see as problematic: citizens will have the opportunity for uncensored access. Over time, they might be persuaded that access to information is a less significant threat to political stability than they previously imagined. Thus, the widespread use of anonymisers may lead indirectly to political change, such that the Chinese Government is less concerned with restricting access to information. In any case, the use of an anonymiser service, while not directly a protest activity, is consistent with Gandhi's requirement to avoid complicity with injustice. And to the extent that anonymisers' widespread use presents the Chinese Government with an opposing reality, it is a legitimate Cyberpunk protest activity.

So far, we have shown that Internet participants treat the online environment as communities to be reformed, not abandoned or replaced, using resources and standards internal to virtual participation. Further, the Gandhian model of non-violent

action grounds a distinction between disobedient reform or resistant activities and malicious or coercive ones. Similarly, we now move to a third incident to demonstrate that the ideas of non-violence and online community provide the necessary theoretical leverage to distinguish the deployment of technological weapons in the service of greater openness from their use to bolster existing power structures.

Denial of Access and File Spoofing

A DoS attack attempts to disable a computer network by flooding it with requests, thereby preventing legitimate clients' effective use of the network. A DoS attack can be executed by those with very limited resources against large and technologically sophisticated organisations. As such, it can be successfully used by Cyberpunks as a form of protest against entrenched power structures. To execute such an attack a Cyberpunk merely needs coding skill, motivation and time, plus minimal computing power (a single old PC) and an Internet connection. DoS attacks were the exclusive domain of Cyberpunks and hackers until organised crime rings adopted DoS attacks as a form of extortion. Thus, the power relation between the attackers and the attacked has altered significantly: it is no longer an 'asymmetric attack' against the strong by the weak. Indeed, a recent development has seen a very strong organisation employ a DoS-style attack against a much weaker opponent.

The extremely well resourced RIAA has employed a DoS-type attack on peer-to-peer (P2P) service providers. This is a new stage in the RIAA's continuing battle with the P2P community. Previously, the RIAA took on P2P service providers like Napster in court. This time, the RIAA has flooded P2P networks with spoofed files with the clear intention of denying users effective access to the service. The spoofed files appear to be those that users have requested, but are instead damaged or otherwise counterfeit, thus making the P2P system unworkable. This use of prima facie Cyberpunk strategies by powerful business interests is a worrying development because of the inversion of the usual power differential. Altnet Inc. filed a lawsuit in the U.S. District Court in Los Angeles in September 2005 accusing the RIAA of infringing an Altnet patent covering technology for identifying requested files on a P2P network. The case was settled in May 2006. Hence in this case, the P2P provider had the resources to seek recompense. But the strategy could be employed against individuals and organizations without such resources. Nevertheless, claiming such Cyberpunk techniques are *only* legitimate when used by the poorly resourced against the well resourced is ad hoc. Fortunately, the model of non-violent action herein endorsed has the necessary theoretical resources to distinguish between uses and abuses of such attacks in a principled, non-ad hoc manner.

On the Gandhian model we have developed, disruptive disobedience is legitimate only to the extent that it is used to confront and challenge entrenched power structures because of identified injustices. The use of DoS-style attacks by the RIAA is being used to retain control against subversive elements – there is no systemic oppression at stake. The present model can ground a morally relevant distinction between the two uses: using cyber strategies to increase exchange and diversity and using the same strategies to entrench control by existing powerful entities. To the extent a disobedient strategy is used to subvert or challenge existing power structures it *may* be legitimate, whereas to the extent that it is used to protect and further reinforce power structures it is illegitimate. The critical factor is whether the Internet's resources are employed as progressive weapons, to maintain and advance the democratic and egalitarian instability online.

This distinction may be available to Google. It is at least plausible to claim that Google's provision of censored material to the Chinese users expands their access. In contrast, in the US, cooperation with government demands for information about users undermines the current status of uninhibited use, and sets a new precedent for restrictions. (At roughly the same time as it signed off on the compromise with China, Google went to court in the US to protect its data from government scrutiny. See the motion filed by Federal prosecutors in January 2006: http://i.i.com.com/cnwk.1d/pdf/ne/2006/google-doj/motion.to.compel.pdf). Opponents would say that the difference for the Chinese users is exaggerated: the Internet community is undermined, and the value of censored access is not sufficient to justify complicity with information oppression. In neither case should a state subvert the net's capacity for the free exchange of ideas, information and knowledge. Again our aim is not to determine whether the Google decision is the morally correct one, but merely to provide a set of conceptual resources whereby this debate can be played out. Gandhian Cyberpunk standards are one way to provide such resources. Still the

debate is not a simple one. For one, it turns on how online groups are to be individuated. Whether one concludes that the Chinese citizen has greater or lesser access to information is partially dependent on the reference group with which they are compared. In comparison to the Chinese citizens prior to the opening of Google.cn the citizens seem better informed; if compared to the average netizen outside China, citizens have impoverished access. Thus, the legitimacy of Google's compromise turns in part on whether the Internet as a whole defines a reference group. This is a complex question, but is not a complexity unique to the online world. For example, should questions of justice that involve comparative welfare and distribution be addressed within nations or between nations? Is the world population as a whole a legitimate reference group?

Non-violent Cyberpunk

Gandhi and his followers are classic examples of civil disobedience in resistance to oppression. Gandhi's emphasis on face-to-face interaction and the importance of placing one's physical being on the line is important. But it is not the only form that truth insistence can take. It seems to us that nothing rules out the use of information and communication technologies in these ways. The critical issue is not the form of interaction, but the aims, results and uses of such interactions. DoS attacks, using illegal anonymous proxy servers and employing hostile technologies can be coercive and violent. Nevertheless, presenting one's case, confronting existing power structures, persisting in disobedient action would be legitimate on the net, just so long as these were aiming for truth, not injustice, and not practiced coercively. Thus, a significant consideration must be the relative level of power exercised. Disruption need not be coercive when the level of power means the disruption is relatively easily overcome and when the intervention undermines or exposes existing coercion. The anonymous server intervention in the Chinese case does not coerce the government, but *may* rather challenge them to reconsider their position and attempt to exercise power. On the other hand, a Cyberpunk undermining of state power or of a commercial monopoly might be disruptive or disobedient, but might ultimately return power to those the status quo does not take into account. Such explicit consideration of state and corporate power is not part of Gandhi's explicit account, but in an age of super states and corporate entities, should be taken seriously

Communities are threatened by individual deviance and by excessive regulation, but conversely, their thriving depends on individual disobedience and some regulatory recourse. A full understanding of net-based communities is threatened when either of these is overlooked: praising Wikipedia as purely anarchic is both misleading as to the structure of the enterprise and misleading as to the value of anarchy. What is good about cyberspace is much the same as what is good in communities anywhere – engagement for fun, for mutual benefit, for education, for collaboration and so on. What is dangerous is manipulation by malicious individuals, corporations or states seeking excessive power over others. Systems for good are those that oppose these abuses of power, including regulatory systems for criminal activities and Cyberpunk interventions against the excesses of such systems. Communities on the net can create themselves as just and cooperative, but can be threatened by individual violations and by powerful political or commercial pressures. Internal regulation is needed to guard against the first and cyber-disobedience the second.

Acknowledgments

Thanks to two anonymous reviewers for SCAN for their thoughtful and constructive comments.

For Tank Man, who many Chinese may never know.

Postscript

Since this paper was accepted for publication two interesting developments have arisen in relation to our claims about the Wikipedia:
1. Larry Sanger co-founder of the Wikipedia, has initiated a rival open-source project, the Citizendium, which aims to "install a responsible approval process and grow to a greater level of maturity as a community" (In Rosencrance 2006)

2. Due to the massive problem of cyber-bullying "next year a new law will come into force which will force Koreans to reveal their name and ID number before they share their opinions online" (Simmons 2006).

References

Anderson, J. (2006) "TIME 100: The People Who Shape Our World - Jimmy Wales: The (Proud) Amateur Who Created Wikipedia", Time.com, http://www.time.com/time/magazine/article/0,9171,1187286,00.html, accessed April 2006

Bender, T. (1982) Community and Social Change in America, Baltimore: Johns Hopkins University Press

de Laat, P. B. (2005) "Trusting virtual trust" in Ethics and Information Technology, vol. 7 no. 3, pp. 167–180

Dreyfus, H. (1999). "Anonymity versus commitment: The dangers of education on the Internet" in Ethics and Information Technology, vol. 1, pp. 15-21

Galston, W. A. (1999) "Does the Internet Strengthen Community?", The Institute for Philosophy and Public Policy, vol. 19 no.4 (1999) http://www.puaf.umd.edu/IPPP/fall1999/internet_community.htm, accessed May 2006

Gandhi, M. K. (2003) "On Satyagraha", in Social and Political Philosophy, ed. J.P. Sterba, 3rd edn, Belmont: Wadsworth

Person, L. (1998) "Notes towards a postcyberpunk manifesto" in Nova Express, Issue 16, reprinted in Slashdot: http://slashdot.org/features/99/10/08/2123255.shtml, accessed May 2006

May, T. C. (1992) "The Crypto Anarchist Manifesto", reprinted in Crypto Anarchy, Cyberstates and Pirate Utopias, ed. P. Ludlow (2001), Cambridge (Mass): MIT Press

McCullagh, G. (2006) "Congress caught making false entries in Wikipedia", C|Net News, http://news.com.com/2061-10796_3-6033082.html, accessed January 2006

Pink, D. A. (2005) "The Book Stops Here", Wired 13:3, http://www.wired.com/wired/archive/13.03/wiki.html?pg=1&topic=wiki&topic_set, accessed March 2005

Racoma, J. A. (2006) "The Truth About Wikipedia", Forevergeek, http://forevergeek.com/fg_commentary/the_truth_about_wikipedia.php, accessed May 2006

Rosencrance, L. (2006) "Wikipedia co-founder to launch competing project", *Macworld*: http://www.macworld.com/news/2006/10/20/citizendium/index.php?lsrc=mwrss, accessed October 2006

Simmons, D. (2006) "Cyber bullying rises in S Korea" BBC News, http://news.bbc.co.uk/2/hi/programmes/click_online/6112754.stm, accessed November 2006

Townley, C. & Parsell, M. (2004) "Technology and Academic Virtue: Student plagiarism through the looking glass" in Ethics and Information Technology, in vol 6, pp. 271-277

Wickre, K. (2006) “Testimony: The Internet in China”, Official Google Blog., http://googleblog.blogspot.com/2006/02/testimony-internet-in-china.html, accessed February 2006

Includes full text of Testimony of Google Inc. *Before the Subcommittee on Asia and the Pacific, and the Subcommittee on Africa, Global Human Rights, and International Operations Committee on International Relations United States House of Representatives.* February 15, 2006. Elliot Schrage Vice President, Global Communications and Public Affairs Google Inc.

Scan is a project of the Media Department @ Macquarie University, Sydney