CYBER-PUBLICS AND THE CORPORATE CONTROL OF ONLINE COMMUNICATION

LINCOLN DAHLBERG

Abstract

The Internet has enabled many individuals and groups to articulate and contest positions on a myriad of local, national, and international issues, thereby extending the public sphere(s) of critical communication at the heart of strong democracy. However, a number of commentators argue that this critical communication is likely to become ever more restricted given the increasing corporate ownership and control of cyberspace. In this paper, I undertake a general investigation of this corporate takeover and the limits it places on the possibility of the Internet extending the public sphere. Focusing primarily upon the United States, I find that the increasing ownership of the network's content, code, and bandwidth by a few huge vertically and horizontally integrated media corporations is providing the basis for the control of online communication. Content discrimination is already being undertaken by some broadband network providers. These trends suggest that the Internet is being developed toward an arena where critical voices and practices will be increasingly marginalised. Given this situation, significant steps will be needed to secure and extend online critical communication. I conclude by suggesting a number of such steps, focusing upon legislative measures that should be urgently considered by Internet researchers and policy makers.

Lincoln Dahlberg is currently an independent researcher in New Zealand, e-mail: L.J.Dahlberg@xtra.co.nz.

Introduction[1]

The Internet is seen by many media theorists as helping extend the public sphere(s) of critical communication believed to be at the heart of strong democracy, involving the open and reflexive articulation and contestation of moral-practical validity claims (or, broadly speaking, political positions).[2] Douglas Kellner (1998, 174), for instance, argues that the Internet has "produced new public spheres and spaces for information, debate, and participation that contain the potential to invigorate democracy and to increase the dissemination of critical and progressive ideas." While showing due caution, other media intellectuals express similar ideas (see Dahlgren 2001; Gimmler 2001). Indeed, there is a huge diversity of communicative interaction taking place online through e-mail, e-mail lists, electronic bulletin boards, online chat, Weblogs, role playing domains, Web publishing and broadcasting, and so on. While much of this communication involves people connecting with others with similar values and interests, there is also extensive critical communication taking place. Through the Internet a great plurality of actors engage in the articulation and contestation of positions on a myriad of local, national, and international issues.

This engagement can be readily found within and between the more "anarchic" spaces of the Internet (Usenet groups, chat, role-playing games). Critical communication is also being extended through the Internet by individuals and groups using e-mail and the Web to articulate and contest positions. Some actors are actually involved in developing online public spaces that aim to support rational-critical interaction and public opinion formation.[3] In addition, there are a plethora of online media that to different extents offer both critical reporting and citizen participation, and thus promise to fulfil earlier hopes that the mass media would offer inclusive spaces of critical publicity. These online media range from the bottom up, "independent" projects (e.g., Weblogs, Independent Media Centre), to the "nonpartisan" professional journalist initiatives (e.g., Opendemocracy.org, Scoop.com), to the expansive portals of the offline established mass media (e.g., CNN, BBC) and new online media companies (e.g., AOL, MSN).

This communication is radically democratic in comparison with the dominant corporate and state controlled mass media, in which content is largely regulated by the owners. While large corporate portals and mass media sites seek to capture online attention for news, information, and interaction, and thus threaten to marginalise critical voices and forms of participation, the Internet continues to provide a space for individuals and groups to articulate and contest any position. However, a number of commentators have warned that the radical democratic promise of the Internet is being threatened by the increasing corporate ownership and control of the Internet (see Barney 2000, 2003; Fortier 2001; McChesney 1999, 2002, 2004; Dahlberg 2002; Schiller 1999). The argument is that powerful corporations supported by neo-liberal policies are taking control of cyberspace and beginning to discriminate in favour of certain voices and practices.

In this paper, I undertake a general investigation of this argument. Focusing particularly upon trends in the United States, I explore the corporate ownership and control of content, code, and bandwidth, and consider the impact of this upon online public discourse. In practice, content, code, and bandwidth are complex and overlapping aspects of the Internet. They are distinguished here simply to

examine different aspects of corporate colonisation of cyberspace.[4] Examples are largely drawn from the United States because it offers an exemplar of advanced (relative to elsewhere) corporate power over cyber-communication under neo-liberalism. From this exemplar, various implications of neo-liberal supported corporate control can be drawn for "the democratic Internet" as a whole, and policy proposals with universal relevance can be developed. In the paper's conclusion, a range of such proposals for expanding critical communication online are put forward for consideration.

Ownership and Control of Content

A few years ago, a number of neo-liberal influenced commentators predicted that the Internet would naturally evolve into an ideal capitalist market of unrestricted trade in information commodities (Dyson et al. 1994; Gates 1995, 1999; Kelly 1998; Keyworth 1997). This expectation has yet to be realised. While some information products – academic journals, private research reports, pornography, financial information, games, software applications – are successfully sold as commodities online, much content is freely distributed on commercial and non-commercial sites, available for anyone (with access to the Internet!) to use and modify as they wish. However, this freedom is now under serious threat. Free online content is being replaced by subscription only services on many media and information sites, as advertising models fail to live up to expectations (hAnluain 2004; Lasica 2003). Moreover, access does not necessarily translate into freedom to copy, share, or redevelop information and software. Online content is increasingly being defined and controlled as private property through law and technology, criminalisation being the result of its "unauthorised" use and distribution.

Promoters of online commerce are now sceptical about the idea that the Internet can support "friction-free capitalism" without state intervention. Instead, they have turned to legislative mechanisms at regional, national, and supranational levels to ensure the online commons of free exchange is transformed into an online free market ruled by the owners of private property (Barbrook 2002; Lessig 2004). On the one hand, agreements are being worked out to keep Internet commerce free of taxes, tariffs, and other regulations that may impede corporate ambitions (Lessig 2001; McChesney 1999). On the other hand, intellectual property rights pertaining to electronic communication are being greatly strengthened. Patents, trademarks, copyright, and anti-hacking laws are being expanded through national legislation and international treaties to ensure the Internet's status as a free market for the sale and distribution of private property (Bollier and Watts 2002; Lessig 2001, 2004; May 2000). Of most concern for democracy is that the "fair use" or "fair dealing" principle that has in many democratic nations ensured public criticism through the use of intellectual property for satire and public education is steadily being eroded, undermining the freedom to engage in critical communication. This erosion of fair use has in some countries (particularly in the United States) reached the stage where corporations are able to deploy intellectual property law to silence online criticism of their operations. Dunkin Donuts, for instance,

> used the threat of a copyright lawsuit to force a site devoted to criticism of the
> [United States] nationwide chain to sell the site to the company. The company
> claimed it could "more effectively capture the comments and inquiries" if it

owned the site. . . . The pattern here is extremely common. Copyright holders vaguely allege copyright violations; a hosting site, fearing liability and seeking safe harbor, immediately shuts down the site (Lessig 2001, 182-193).

Trademark law is similarly being deployed to silence criticism. As Bollier and Watts (2002, 47) report, "many companies have used trademark claims to shut down websites that use their name in a disparaging way, as in 'walmartsucks.com' and many other 'sucks' sites." Trademark law has increasingly been used by corporations to claim domain names, as well as brand names, as private property. Thus, the reach of private property relations is being extended deeper into cyberspace, which is further constituted as space for free trade rather than free speech. At the international level, quasi-governmental organisations have supported this extension of trademark law to cover domain names. For example, The World Intellectual Property Rights Organisation's deliberations over Internet addresses, involving mostly large firms meeting behind closed doors, have favoured corporate interests over the public (Sassen 2000). The Internet Corporation for Assigned Names and Numbers (ICAAN), which is responsible for domain name registration and dispute resolution, has consistently ruled in favour of those companies who own trademarks over domain name holders and other non-profit contenders (Bollier and Watts 2002, 48).

However, media corporations are not simply relying on the application of traditional legal mechanisms to control online content. They are also developing new licensing and software systems to curtail the remaining fair public use principles and eliminate the already many-times extended limits on the terms of intellectual property rights (Lessig 1999, 2001, 2004; Shapiro 1999). Perpetual ownership and control of content is being attempted through application of aggressive licensing systems ("shrink-wrap" licenses for software, "click-through" licenses on Websites)[5] and digital rights management technologies (Bollier and Watts, 2002; Lessig 2001, 2004). This attempt to eliminate fair use rights and the limits on copyright terms of digital materials is being backed up by new laws, including law criminalizing the act of breaking the code of copyright management systems and even law prohibiting the development of software that could be used to break such code. The most draconian example of such law (so far) is the United States' 1998 Digital Millennium Copyright Act (DMCA). This law prohibits the writing, sale, and use of software that could circumvent any technical measure controlling access to a copyrighted work. It has already been employed to prosecute detected breaches of corporate controls. Corporations have successfully taken legal action against developers of technology that simply makes purchased software more user-friendly and against researchers of security systems that point out problems with those systems (Bollier and Watts 2002, 46-47; Lessig 2001, 2004).

One classic example is the arrest of the twenty six year old Russian programmer Dmitry Sklyarov who had disclosed encryption flaws in e-book software made by Adobe. Sklyarov was arrested at the 2001 DefCon hackers conference after giving a talk on unlocking electronic books. He and his employer, ElcomSoft Co. Ltd., were charged with violating the DMCA by writing and selling a program that allowed users of Adobe Systems Inc. e-Book Reader to bypass copyright protection code (specifically to decode and read e-books written by Adobe products). Skylarov was eventually released and allowed to return to Moscow with the promise that

charges against him would be dropped if he served as a witness in the case against ElcomSoft. A Federal court jury eventually found in favour of ElcomSoft. However, this finding does not represent a significant challenge to the DMCA and its support for the indefinite extension of copyright through code. The trial jury actually agreed that ElcomSoft's product was illegal. The company was only acquitted because the jury believed that ElcomSoft did not wilfully violate the law, and, in fact, under cross examination an Adobe engineer acknowledged that his company had not found any illegal e-Books resulting from ElcomSoft's product (i.e., they had all been purchased before being cracked).

Information property law, licenses, and information protection systems are threatening to limit the freedom to access and use online information for the critical communication and cultural creativity central to strong democratic culture. Cyberspace is moving toward a sphere of commodity exchange and instrumental action rather than a sphere of communicative action, it is developing into a consumer centric rather than public centric space. Yet legal restrictions, licenses, and digital rights management technologies are also being circumvented by the practices of thousands of Internet users, who are swapping copyrighted material and breaking information protection systems on a daily basis (Dyer-Witheford 2002; Jordan and Taylor 2004). Media corporations (often with state assistance) are searching for new ways to carry out wide ranging and effective network surveillance that would deter such "criminal" behaviour (Barbrook 2002). So far, such surveillance has not been successful. The few high profile prosecutions that have been effected have not deterred everyday users from copying and sharing information and cracking code. This situation may change if surveillance systems are greatly improved and users believe that there is an increased chance of being caught. At present, the Internet provides for the free use, re-development, and re-distribution of extensive information, and it offers a means for public critique of the very corporations and governments that are trying to control content. However, corporate control of Internet content and practice is developing at a "deeper" level than copyright and copy protection: It is developing through the ownership of network code and bandwidth.

Ownership and Control of Code

A central element in claims about the Internet's democratic nature is the fact that its architecture has supported non-discriminatory communication. However, the increasing privatisation of the Internet's code (operating and applications software) is allowing corporate structuring and control of online communication. The commercial design and corporate control of significant Web properties, distribution mechanisms, and applications software – aimed to capture users for advertising and sales – is structuring much online public space for consumer practices rather than for democratic communication (Hargittai forthcoming; Patelis 2000; Dahlberg forthcoming). Yet the Internet continues to provide support for vibrant critical communication outside commercially structured spaces. More significant for "the democratic Internet" than the commercial colonisation of Web space is the increasing corporate ownership and control of the network's operating software, which threatens to limit the Internet as a free and open communication system.

Some commentators argue that the "end-to-end" network architecture princi-

ple has been responsible for the Internet's non-discriminatory nature. Unlike broadcasting, where the system's intelligence is centralised within the network, the Internet was architectured to be "stupid," with all its intelligence at the ends, meaning that the network itself could not "discriminate." In other words, the Internet technology was designed to be neutral to all content, applications, and innovations carried over it (Bollier and Watts 2002, 26-27; Lessig 2001). Thus follows the (somewhat technologically determinist) argument that this architecture must be retained in order to guarantee non-discriminatory communication. However, as Sandvig (forthcoming) points out, nondiscrimination does not rely upon having an end-to-end system. Fundamental elements of online communication have not been end-to-end and yet have largely been sustained as non-discriminatory. For instance, e-mail has for a long time used intermediaries to cache and distribute mail, and Web pages have been held on centralised servers rather than individual computers. Those with access to the intermediaries could in principle survey and edit e-mails and Web pages, but they have largely allowed the free flow of communication due to socio-cultural rather than technological reasons.

For a start, common carrier law (to be further considered below) has helped enforce the free flow of data. Moreover, a mixture of semi-formal *social* code (public licensing systems) and informal *cultural* code (the Internet's open ethos) has contributed to an open system. In any case, the end-to-end form does not guarantee non-discrimination. Although end-to-end may make discrimination more difficult since the technology *within* the system is "stupid," discrimination can still take place at the network's ends through regulations and restrictions on what can be carried. Thus, it is not the form of the network that has secured its openness, but the fact that this form has been placed in the public domain by a combination of formal law, semi-formal social codes, and informal cultural agreements that have been adhered to by the majority of contributors to the network's development.[6] The significant threat to the Internet's democratic promise is not changes to its technological form, although such may mean more possibilities for discrimination. The significant threat is the increasing corporate ownership and (largely) unregulated control of the evolving network architecture.

The Internet's most fundamental technical code (including the TCP/IP set of protocols behind the end-to-end architecture) remains in the public domain (non-proprietary and open source),[7] allowing for the nondiscriminatory transmission of data, the attachment of any computing device to the network (given technical compatibility), and the modification of the protocols as needed. In addition, much of the important software that is layered on top of the TCP/IP protocols and that makes the present network operate is also in the public domain (WWW protocols of HTTP and HTML, Apache Web server, Linux operating system, BIND DNS server). However, significant new software of the evolving Internet architecture, from operating systems to Web browsers, is proprietary and closed (hidden from view and protected by copyrights and patents). Companies behind this new software, and associated systems, are now engaged in battle with each other and with open source software to determine future technical standards, including standards for online communications media (such as instant messaging, e-books, audiovisual, wireless systems, online telephony, etc), platforms (browser and desktop software), and associated equipment (set-top boxes) (Bollier and Watts 2002; Lessig 2001, 2004).

The problem here for "the democratic Internet" is that closed and proprietary standards will not only limit democratic innovation but will also facilitate corporate control of online data flows – a small number of large profit-oriented corporations determining what content and applications are allowed. This would favour commercial rather than critical forms of communication.

Various non-profit Internet governance organisations – such as the World Wide Web Consortium (W3C) and the Internet Engineering Task Force – are presently deliberating on future standards. These organisations are in theory "open to all interested participants and work in an informal, deliberative manner that favours technical efficiency and open, non-proprietary Internet architecture" (Bollier and Watts 2002, 27-28). However, in practice these groups tend to bias industry and government players over public groups (by, for instance, making membership very costly) (Salter 2003). They are also under increasing pressure from corporate interests to endorse proprietary standards for the Internet (Bollier and Watts 2002, 28). In any case, the recommendations of these organisations are not binding (ibid). Moreover, companies like Microsoft are not waiting on "independent" deliberations to decide future standards. Microsoft and other major players are deploying a plethora of strategies in order that their software gains the degree of dominance that will achieve the status of de facto proprietary standard(s). These strategies not only include the takeover or elimination of innovations and competitors, but also the formation of corporate lobby groups and strategic agreements. For instance, Microsoft has joined forces with IBM, Intel, and BEA systems to set up a consortium to "complement" the W3C (ibid). Microsoft has even entered a cooperative agreement with its one time archenemy AOL (owner of Netscape), which allows each to support the other (rather than going loggerheads in court as they have previously) in the domination of their respective areas of the Internet market – software and media content respectively (Lohr and Kirkpatrick 2003).

Through such strategies, Microsoft is rapidly moving toward having its various software established as de-facto Internet standards and thus being able to extensively structure and control online communication. More than 90 percent of Internet browsers installed on personal computers are now versions of Microsoft's closed Explorer software, which is supported by its dominant desktop platform. Through its latest platform, the Windows XP & .NET products, Microsoft aims for total control of Internet use by bundling together its operating system, Web browser, Internet service provision, and online applications. Those Internet services and application providers that are not simply shut out because they pose a direct competitive threat to Microsoft's dominance need to more than ever design their technologies according to Microsoft's technical code.

Microsoft presently faces resolute competition from the open source software movement. In order to defeat this threat to its dominance,

> Microsoft has adopted a policy of "embrace, extend, and extinguish" toward open-source software. The company adopts a free and publicly accessible program, adds wrinkles that allow it to copyright a new version of the program, and then makes only its copyrighted version compatible with its other products, such as Windows. It has used this strategy to undermine HTML; Java, the versatile programming language; and multimedia applications such as RealAudio, and QuickTime (Levine 2002, 15-16).

Microsoft has also discounted its software in Europe for government and large private agencies and has dramatically increased its donations to non-profit organisations, all in aid of countering the spread of open-source programs (Markoff 2003). Microsoft is just one of a number of players driving the Internet's applications and operating software, and thus content and services, toward centralised, private control. This control is likely to lead to a substantial limitation on critical online communication – corporations are likely to favour profit-oriented technologies and content, and to develop the Internet's architecture so as to foster a consumer-oriented rather than citizen-oriented cyberspace. Another significant way in which this move toward centralised, corporate control is taking place is via the increasing role that unregulated, broadband networks are taking in providing Internet bandwidth.

Ownership and Control of Bandwidth

A central reason for the Internet operating as a non-discriminatory network is the fact that data has been carried over telephone systems that in the United States and many other nations are accorded common carrier status. Under these rules, network suppliers have been prohibited from interfering with online communication and from limiting what devices and applications can be carried on the network. This has not stopped Internet service providers structuring online experience so as to channel users to their own or allied content. However, common carrier rules have ensured that (in many countries) all legal content and applications are actually carried online.

This non-discriminatory network situation is changing with the development and spread of Internet broadband access and content services carried by communication networks (cable, wireless, satellite, DSL[8]) that are not generally regulated as common carriers. This gives bandwidth providers the opportunity to discriminate. In a situation of multiple independent service providers (e.g., when open network regulation is applied),[9] discrimination by a particular carrier *may* not be such a problem. However, these broadband networks are largely owned by a few huge and increasingly dominant communications corporations, which are also media content companies and thus have particular interest in the actual information and applications they carry (Bagdikian 2000; McChesney 2002).[10] The result is not just the possibility but the increasing practice of corporate regulation of Internet communication. Network service providers can combine various content and software control mechanisms to regulate what is carried over their lines. For instance, they now deploy "acceptable use policies" to reserve for themselves the right to discriminate. To assist such discrimination, network technology developers like Nortel and Cisco are designing intelligence capabilities into new broadband systems (Winseck 2002, 805-806). Referring to Cisco documents, Winseck (2002, 806) explains that "in essence, gate-keeping functions have been hardwired into network architectures as part of the communications industries' strategies to cultivate and control markets." Some network owners, particularly cable operators in the United States, have already carried out actions restricting Internet use (in addition to pointing subscribers to certain content and services via start-up portal sites). These forms of restriction include:

- Restricting or prohibiting users from access to Internet content, including access to other ISPs and Wi-Fi services (Greene 2004; Saltzer 1999).
- Restricting users from running certain applications. This includes limiting the use of applications that undermine the network provider's commercial operations, such as applications that block advertising, cookies, and identification of e-mail addresses. Some network owners are restricting the use of competing Internet services. For instance, a number of cable companies have prohibited subscribers using internet telephony, home Websites, and file sharing, and have limited the time that users can stream video from the Internet (Bollier and Watts 2002, 33; Oakes 2000; Winseck 2002, 809).
- Applying quality of service differentiation that directs attention toward certain content and services, and away from others. For instance, Cisco's intelligent network technology can be used to point users to a network's own products and affiliated services, and away from that of competitors, by allocating greater or lesser bandwidth and thus changing relative performances (Lessig 2001, 46).
- Prohibiting attachment of devices to an Internet connection. For instance, some network providers have refused to attach home networks (made up of two or more computers, televisions, Wi-Fi routers, and other devices) to the Internet (Greene 2004; Oakes 2000; Saltzer 1999). In other words, they have refused to carry traffic to and/or from Internet addresses that they did not assign, which prevents customers from contracting for simultaneous service with any other Internet provider.
- Restricting users adding or delivering content (ibid). Such restrictions encourage consumption of content rather than the production and distribution of materials by the user, which undermines the synchronous and democratic form of the network. More subtly, network providers can discourage outbound traffic flows by charging high prices for such data transmission. This overlaps with the next aspect of control.
- Applying tiered levels of Internet service delivery that excludes or discourages some forms of online communication. In many (poorer) locations network service providers deem it unprofitable to install the technology for, and undertake the supply of, any more than limited Internet bandwidth. Moreover, where broadband service is provided, content and services may be offered on a pay-per-service or pricing scheme basis, ranging from free access for a packaged deal of largely commercial content, to extensive Internet content, interactivity, and upstream data delivery through high speed Internet (Chester 2002). Winseck (2002, 809) gives a list of such pay-per service options that AT&T's excite@Home service (now taken over by Comcast) offers, including charges for the operation of a news service, email distribution, and bulk mailing of messages (including information announcements, charity requests, petitions for signatures and political or religious messages). These service differentiations, along with the other content discriminations discussed above, are transforming the Internet into a one-way broadcaster for those who do not have the means or desire to pay high rents or who live in the "wrong" locations.

Further discriminatory possibilities are offered to network owners with the development of smaller and dumber devices like cell-phones. Unlike desktop

computers with their own computing power and memory, these devices rely upon the intelligence of a mainframe computer and technological arguments may in the future be used to legitimate content discrimination (Levine 2002, 6). This discrimination will no doubt favour the interests of the media corporations who own the mobile devices, the transmission systems, and (often) the content. These companies "will be able to steer their customers to certain services and Web pages" (ibid). For some users the Internet could be reduced to a relatively small set of commercially chosen Web products. The result will be a fully managed "walled garden," a monopolisation of the digital audience by major corporate interests.

Deregulatory environments around the world are encouraging these developments. While some regulations have been applied, they have largely been in aid of encouraging open competition to advance the information economy rather than for advancing democratic ideals (Sallet 2003). Without common carrier and strong cross-ownership rules, the broadband future looks to be one of editorial control by a few dominant corporate network suppliers. Soon it may not only be a challenge to attract online attention; it may be difficult to actually get one's message (particularly if oppositional to dominant ideologies) carried by those who own the lines.

Extending Critical Communication through the Internet

The Internet provides a space through which civil society groups and individuals can articulate and contest common problems and concerns. However, the general exploration undertaken in this paper indicates that, in the case of the United States most specifically, a few corporations are increasingly gaining ownership of the Internet's content, code, and bandwidth, and thus the power to determine what can be accessed and communicated online. The threat is that the Internet will become another corporate controlled media, with critical communication marginalised or completely excluded and users constituted as consumers rather than critical-reflexive citizens.

I want to briefly put forward for consideration a number of regulatory-focused proposals for how online critical communication may be protected and extended. These proposals are intended to be globally applicable. The focus upon United States examples in this paper has universal relevance not only because Internet developments are not contained by international borders but also because the case of the United States demonstrates how corporate control operates under neo-liberalism. I concentrate on regulatory solutions rather than technological solutions because, without the former, any technical developments that threaten corporate domination are likely to be sidelined, blocked, or appropriated. Legal protection of the existing open network is urgently needed not only so that it can continue to exist but also so that it can develop democratically.

In terms of the corporate control of content, copyright and related licensing must be reformed to provide for democratic use. First, legislation is needed to reduce the length of copyright and provide for extensive "fair use" of creative works. Second, legislation (or in some cases a repeal of legislation) is needed to ensure that licensing and digital rights management schemes are prohibited from perfecting control (expanding copyright indefinitely) and undermining the public's right to "fair use." Third, those who support a democratic Internet need to promote open forms of licensing that permanently place works in the public domain while giv-

ing recognition to the creators. Examples of such licensing include Lawrence Lessig's Creative Commons, the Electronic Frontier Foundation's Open Audio License for music in digital formats, the French visual artist's initiated "Arts Libre" or "Free Art" license for digital images, and the "Open Content License" and "Design Science License" drafted as all-purpose licenses that could place any type of creative work in the public domain (Bollier and Watts 2002, 50-51).

At the level of network software, official bodies and organisations need to promote open, non-proprietary code and technical standards. First, strong support from government and civic organisations must be given to open source licensing as embodied in the General Public License of the Free Software Foundation.[11] One way public bodies can provide such support is by purchasing and installing open source licensed software for their systems. A number of governments – China, Brazil, Japan, South Korea, city of Munich – have already, for various reasons, decided to use and develop open source software. Second, there needs to be greater government and civil society backing for the work of the non-profit standards setting organisations so that open technical standards are maintained. Bodies such as the Internet Engineering Task-force and the World Wide Web Consortium have been effective in the past in this endeavour, but need to be further democratised and, in the face of industry pressures need stronger support and involvement from democratic bodies and non-profit public interest groups (Bollier and Watts 2002, 32).

At the level of bandwidth, legislative provisions are needed to ensure a non-discriminatory network. First, the Internet must be accorded common carrier status to ensure no discrimination of content, services, or applications by network owners and service providers. This means that all network owners (cable, satellite, wireless, terrestrial) must be open to carry all ISPs, including competitors at suitable rent. Moreover, it means that all ISPs must provide access to all content (apart from de-humanizing content) available on the Internet, with clearly marked exit routes, out of ISP start-up pages and managed content areas.[12] Second, legislation is needed to maintain and strengthen media cross-ownership and anti-monopoly laws to ensure pluralism of Internet access routes and media sources. Third, significant portions of the radio spectrum must be left in the public domain to encourage the development of public wireless networks and thus further safeguard open Internet access (see Lessig 2001, 241-243). Fourth, legislation is needed that provides for universal and low-cost service of two-way digital networks, rather than tiered services for different groups on the basis of consumer power. As the Center for Digital Democracy argues, universal service requirements should be updated to include advanced telecommunications services.[13]

All these solutions need to be further investigated in terms of their particular and combined impact in order to develop detailed and workable proposals on how to best secure and expand online critical communication. First, the particular forms of regulation need further debate and research. This debate can be fully developed now that the rhetoric that the Internet cannot or should not be regulated has been largely disposed of as ideological – given the Internet has always been regulated through, for instance, target funded and subsidised network development, information property laws, indecent publication laws, surveillance laws and corresponding systems, and the terms and conditions set for the provision of communication services generally. The question is not can or should we regulate the Internet. The

question that needs to be asked and researched is the type of regulation to best apply to maximise public communication given the global and decentralised nature of the medium. This includes consideration of the type of governing bodies that should be involved in regulation. As well as national level governance, international governing bodies, including those mentioned above, need to be democratised and given greater power to oversee the development of the Internet as a global space of citizen communication. Second, the best combination of solutions for maximizing diversity of voice and encouraging critical practice does not simply depend on future technological and social developments, but on the specific legislative measures that are, or are not, applied. For instance, if common carriage is not applied, then strong public service type rules will be necessary to safeguard and promote the articulation of diverse views and the critical contestation of positions.

The above proposals may seem unlikely to be taken seriously given the present alliance between neo-liberal government and powerful corporations, and given the general ideological climate celebrating consumer sovereignty, free markets, and technological solutions. For significant advancement of any of the proposals put forward above, a stronger understanding and commitment to democratic communication is needed amongst policy makers and the general public. To bring this about, radical publics challenging corporate control of systems and articulating democratic ideals for communications media are required. Such publics do presently exist, as indicated by some of the academic and citizens groups referred to in this paper. These groups are working hard to broaden public understanding and debate about, and subsequently resistance to, the privatisation and closure of the Internet's infrastructure. As such, these publics provide the basis for mobilizing support for policies that limit the corporate threat to the Internet extending public sphere(s), a mobilisation that for success needs further backing and resources from critical intellectuals and democratically-oriented civic organisations.

Notes:

2. The public sphere conception here draws upon a critical reading of Habermas (1996). Such a critical reading can be drawn from the likes of Dryzek (2000), Kellner (2000), Matustík (1998), and Young (2000).

3. Exemplary United States based Internet initiatives that aim to actively facilitate citizen deliberation include Kuro5hin, E-ThePeople.org, Politalk.com, and Minnesota E-Democracy.org.

4. The differentiation here between content, code, and bandwidth, should not be confused with the layer models deployed in Internet design. For a brief description of these layer models see Connected: An Internet Encyclopedia, Protocol Layering

(http://www.freesoft.org/CIE/Topics/14.htm).

5. With "shrink wrap" and "click through" systems, agreement with a license is assumed to follow from the purchase of a piece of software or by clicking on a Website displaying the licence.

6. See Sandvig (forthcoming) for an excellent discussion of the end-to-end debate, which demonstrates that it is not technological attributes but norms of openness, transparency, participation, etc., that have sustained the Internet's non-discriminatory communication.

7. Open source, here, means any software for which the source code is open to be read, altered, and redistributed, with new versions then available for further user modification.

8. Digital subscriber line (DSL) transmits broadband through telephone lines and, as such, is automatically regulated as a common carrier in many countries. However, under deregulatory regimes (in the North America, Europe, Oceania), DSL is being relieved of common carrier rules (Sallet 2003, 30-39).

9. There is much talk in Internet economics of instituting open network regulation in order to protect consumers (rather than citizens) from service discrimination. But an open network, in the sense of networks open to all competing content suppliers, does not guarantee common carriage. Competition does not ensure non-discrimination. Certain content, such as criticism of media advertising, may be excluded or sidelined by all competitors. Common carrier rules are thus needed to protect the non-discriminatory flow of content in both monopoly situations and open networks.

10. The Columbia Journalism Review gives a United States focused overview of "who owns what" at http://www.cjr.org/tools/owners/. The Center for Digital Democracy monitors broadband ownership and public policy developments in the United States, and provides analysis of the corresponding limits these developments have upon online democratic communication. See http//www.democraticmedia.org/index.html.

11. "The [General Public] license grants anyone the freedom to use, modify and redistribute the [publicly licensed] software however they wish on the condition that the identical license terms apply to any future distributions of the software" (Bollier and Watts 2002, 49). This ensures the software remains in the public domain.

12. This second part of the common carrier requirement – non-discrimination towards content – is often neglected in current discussion of open networks due to the assumption that commercial ISP competition will provide for common carriage.

13. See the Center of Digital Democracy's Declaration of Digital Democracy http://www.democraticmedia.org/issues/decDigitalDemocracy.html

References:

Bagdikian, Ben H. 2000. *The Media Monopoly*. Boston: Beacon Press.

Barbrook, Richard. 2002. The Regulation of Liberty: Free Speech, Free Trade and Free Gifts on The Net. *Science as Culture* 11, 2, 155-170.

Barney, Darin. 2000. *Prometheus Wired: The Hope for Democracy in the Age of Network Technology.* Sydney: UNSW Press.

Barney, Darin. 2003. Invasions of Publicity: Digital Networks and the Privatization of the Public Sphere. In Law Commission of Canada (ed.), *New Perspectives on the Public/Private Divide,* 8-22. Vancouver: University of British Columbia Press.

Bollier, David and Tim Watts 2002. *Saving the Information Commons: A Public Interest Agenda in Digital Media*. New America Foundation. Retrieved March 21, 2004, from http://www.newamerica.net/Download_Docs/pdfs/Pub_File_866_1.pdf.

Chester, Jeff. 2002. The Death of the Internet: How Industry Intends to Kill the 'Net as we know it. *TomPain.Common Sense* (24 October). http://www.tompaine.com/feature.cfm/ID/6600/view/print.

Dahlberg, Lincoln. 2002. Democratic Visions, Commercial Realities? The Corporate Domination of Cyberspace and the Prospects for Online Deliberation. *AntePodium, April*/http://www.vuw.ac.nz/atp/articles/Dahlberg_0204.html.

Dahlberg. Lincoln. Forthcoming. The Internet as Public Sphere or Culture Industry? From Pessimism to Hope and Back. *Media and Cultural Politics* 1, 1.

Dahlgren, Peter 2001. The Public Sphere and the Net: Structure, Space, and Communication. In

L. W. Bennett & R. M. Entman (eds.), *Mediated Politics: Communication in the Future of Democracy,* 33-55. Cambridge: Cambridge University Press.

Dryzek, John S. 2000. *Deliberative Democracy and Beyond*. Oxford: Oxford University Press.

Dyer-Witheford, Nick. 2002. E-Capital and the Many-Headed Hydra. In G. Elmer (ed.), *Critical Perspectives on the Internet,* 130-163. Lanham, Maryland: Rowman & Littlefield.

Dyson, Esther, George Gilder, George Keyworth, and Alvin Toffler. 1994. *A Magna Carta for the Knowledge Age.* The Progress and Freedom Foundation. Retrieved April 19 2004 from http://www.pff.org/publications/ecommerce/fi1.2magnacarta.html.

Fortier, François. 2001. *Virtuality Check.* London: Verso.

Gates, Bill. 1995. *The Road Ahead.* New York: Viking.

Gates, Bill. 1999. *Business @ The Speed of Thought: Using a Digital Nervous System.* New York: Warner Books.

Gimmler, Antje. 2001. Deliberative Democracy, The Public Sphere and the Internet. *Philosophy & Social Criticism* 27, 4, 21-39.

Greene, Thomas C. 2004. Tech Heavyweights Explain How to Destroy the Internet. *The Register* (1 April). Retrieved April 20, 2004 from http://www.theregister.co.uk/2004/04/01/tech_heavyweights_explain_how.

Habermas, Jürgen. 1996. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy.* Translated by William Rehg. Cambridge: Polity Press.

hAnluain, Daithi. 2004. Free Content Becoming a Thing of the Past for UK's Online Newspaper Sites. *Online Journalism Review* (13 February). Retrieved February 20, 2004, from http://www.ojr.org/ojr/business/1067472919.php.

Hargittai, Eszter. Forthcoming. The Changing Online Landscape: From Free-For-All to Commercial Gatekeeping. In P. Day and D. Schuler (eds.), *Community Practice in the Network Society: Local Actions/Global Interaction.* New York: Routledge.

Jordan, Tim and Paul A.Taylor. 2004. *Hacktivism and Cyberwars: Rebels With a Cause.* London: Routledge.

Kellner, Douglas. 1998. Intellectuals, the New Public Spheres, and Techno-Politics. In C. Toulouse and T. W. Luke (eds.), *The Politics of Cyberspace: A New Political Science Reader,* 167-186. New York: Routledge.

Kellner, Douglas. 2000. Habermas, the Public Sphere, and Democracy: A Critical Intervention. In L. E. Hahn (ed.), *Perspectives on Habermas,* 259-287. Peru, IL: Open Court.

Kelly, Kevin. 1998. *New Rules for the New Economy: Ten Ways the Network Economy is Changing Everything.* Fourth Estate: London.

Keyworth, George. A. 1997. *People and Society in Cyberspace, the Shape of Things: Exploring the Evolving Transformation of American Life.* Progress and Freedom Foundation. Retrieved October 21, 2003 from http://www.pff.org/tsot-1.html.

Lasica, J. D. 2003. Are Digital Newspaper Editions More than Smoke and Mirrors? *Online Journalism Review* (4 June). Retrieved February 20, 2004, from http://www.ojr.org/ojr/technology/1054780462.php.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace.* New York: Basic Books.

Lessig, Lawrence. 2001. *The Future of Ideas: The Fate of the Commons in a Connected World*. New York: Random House.

Lessig, Lawrence. 2004. *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: The Penguin Press.

Levine, Peter. 2002. Building the Electronic Commons: A Project of the Democracy Collaborative. Retrieved April 10, 2004, from http://www.democracycollaborative.org/ programs/public/BuildingElectronicCommons.pdf.

Lohr, Steve and David D. Kirkpatrick. 2003. AOL Time Warner and Microsoft End a Bitter Rivalry. *The New York Times,* 30 May.

Markoff, John. 2003. Microsoft Finds Some Doubters for the Motives of its Largesse. *New York Times,* 26 May.

Matustík, Martin J. B. 1998. *Specters of Liberation: Great Refusals in the New World Order*. Albany: State University of New York Press.

May, Christopher. 2000. *A global Political Economy of Intellectual Property Rights: The New Enclosures?* London: Routledge.

McChesney, Robert W. 1999. *Rich Media, Poor Democracy: Communication Politics in Dubious Times.* Urbana: University of Illinois Press.

McChesney, Robert W. 2002. The Titanic Sails On: Why the Internet Won't Sink the Media Giants. In G. Dines and J. Humez (eds.), *Gender, Race and Class in Media,* 667-683. London: Sage.

McChesney, Robert W. 2004. *The Problem of the Media: U.S. Communication Politics in the Twenty First Century*. New York: Monthly Review.

Oakes, Chris. 2000. Cable Net Users Feel Squeezed. *Wired* (18 August). Retrieved April 20, 2004, from http://www.wired.com/news/technology/0,1282,38227,00.html.

Patelis, Korinna. 2000. E-Mediation by America Online. In R. Rogers (ed.), *Preferred Placement: Knowledge Politics on the Web,* 50–63. Masstricht: Jan van Eyck Akadamie.

Sallet, Jonathan. 2003. Just How Open Must an Open Network be for an Open Network to be Labeled "Open"? *FirstMonday* 8m 3. Retrieved January 20, 2004, from http://firstmonday.org/issues/issue8_3/sallet.

Salter, Lee. 2003. The Internet: Potentiality and Limits. Paper presented at Workshop on The Internet: Structure and Use (3 September). London: Metropolitan University.

Saltzer, Jerome H. 1999. *"Open Access" is Just the Tip of The Iceberg*. Retrieved October 21, 2003, from http://web.mit.edu/ Saltzer/www/publications/openaccess.html.

Sandvig, Christian. Forthcoming. Shaping Infrastructure and Innovation on the Internet: The End-to-End Network that Isn't. In D. Guston & D. Sarewitz (eds.), *Shaping Science and Technology Policy: The Next Generation of Research*. Madison: University of Wisconsin Press. Draft Retrieved July 2004, from http://www.spcomm.uiuc.edu/users/csandvig/research/Communication_Infrastructure_and_Innovation.pdf.

Sassen, Saskia. 2000. Digital Network and the State. *Theory, Culture & Society* 17, 4, 19-33.

Schiller, Dan. 1999. *Networking the Global Market System*. Cambridge, Mass: MIT Press.

Shapiro, Andrew. 1999. *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World as We Know It.* New York: Public Affairs.

Winseck, Dwayne. 2002. Netscapes of Power: Convergence, Consolidation and Power in the Canadian Mediascape. *Media, Culture & Society* 24, 6, 795-819.

Young, Iris M. 2000. *Inclusion and Democracy*. Oxford: Oxford University Press.