Pedagogies of Digital Citizenship and the Politics of Code

Graham Longford
University of Toronto

"Tiny controls, consistently enforced, are enough to direct very large animals" (Lessig 1999).

"…control of code is power. For citizens of cyberspace, computer code…is the medium in which intentions are enacted and designs are realized, and it is becoming a crucial focus of political contest. Who shall write the software that increasingly structures our daily lives? What shall that software allow and proscribe? Who shall be privileged by it and who marginalized?" (Mitchell 1995).

"[I]nformation technology…entails more than computers, programmes, fibre-optic cables, mobile telephones and so forth. *Every technology also requires the inculcation* of a form of life…" (Rose 1999).

Introduction: Technological Citizenship in the Digital Era

The rapid development and proliferation of new information and communication technologies (ICTs) has given rise to lively debate and a growing literature on technological citizenship in the digital era addressing topics ranging from e-democracy, networked social movements, and the digital divide, to the virtual public sphere, and electronic surveillance. This essay adopts a somewhat uncommon approach to the question of citizenship in the era of digital technology, one which highlights the ways in which citizenship norms, rights, obligations and practices are *encoded* in the design and structure of our increasingly digital surroundings. To be more specific, it explores technological citizenship in terms of the ways in which, particularly at the level of technical design, the Internet and the World Wide Web regulate and *govern* users, enabling and cultivating certain conduct, activities, and forms of life while simultaneously constraining and neutralizing others. Cyberspace, while often described erroneously as lawless and anarchic, is governed by its technical infrastructure and supporting features which simultaneously enable and constrain users. In other words, there is a *politics of code*; in so far as Internet architectures and software code *legislate* questions regarding how the Internet and the web are used, by whom, and under what conditions (Lessig 1999, 6; 20). Such technical features encode what Luke calls "hidden pedagogies of citizenship" into the

architecture of the Internet and the web, shaping users' conduct, habits and experiences on-line (Luke 2002). To the extent that Internet users are subject to law-like codes regulating on-line behaviour and access to information, our understanding of technological citizenship in the digital era must transcend preoccupations with the digital divide, electronic voting and the like, to interrogate the terms of technological citizenship as they are encoded in cyberspace. Genuine technological citizenship in the digital era entails a critical awareness of how code constitutes the conditions of possibility for different norms, models, and practices of on-line citizenship, along with the capacity to resist and reshape—to *hack*, if you will—the prevailing terms and conditions of cybercitizenship if they no longer serve our needs.

ICTs, citizenship and democracy

A number of influential approaches to technological citizenship have emerged out of the rapidly expanding literature on the information society, e-democracy, networked social movements, and the virtual public sphere. A large body of work emphasizes the appropriation of new ICTs by various agents (social movements, political parties, and governments) for the purposes of disseminating information, facilitating communication, and organizing and mobilizing supporters (Barney 1996; Diebert 2003; McCaughey and Ayers 2003; Norris 2002; Wilhelm 2000). Much of this work focuses on the use of ICTs as tools to renew or enrich existing democratic practices and institutions. Major questions revolve around quantitative and qualitative issues, such as the degree to which ICTs recruit new participants to the political process or merely reinforce the activities of those already engaged (Norris 2002). The qualitative impact of new ICTs is taken up in lively debate and discussion of the virtual public sphere, which focuses on the depth, diversity, and conduct of online political deliberation among citizens (Hill and Hughes 1998; Poster 1995; Sunstein 2001).

Another approach focuses on communicative rights and liberties, examining both the expansion and curtailment of traditional civil liberties, such as freedom of expression and the right to privacy, in the context of digital technologies. While some celebrate the ways in which the Internet promotes freedom of expression and the exchange of ideas and information (Negreponte 1995; Lévy 2001), others have traced its connection to media industry trends, such as technological convergence and corporate consolidation, which have reduced media diversity and access to alternative voices (McChesney 1999; Schiller 1996). Developments in new ICTs have also spawned the burgeoning field of surveillance studies,

which traces the social and political effects of increasingly ubiquitous forms of electronic surveillance (Ball and Webster 2003; Lyon 2001)

Another important strand of research on technological citizenship stems from the literature on the political economy of the information society, "global cities," and high-technology "clusters" like Silicon Valley. Such work focuses on the economic and social impact of industrial change from Fordism to post-Fordism, under which certain places, industrial sectors and populations (both outside and within the new economy) are valorized while others are marginalized (Barney, 2000; Castells 1989; Mosco & Schiller 2001; Murdock & Golding, 2001; Robins & Webster 1999; Sassen 1998). According to this body of work, the significance of new ICTs for democratic citizenship cannot be divorced from the political-economic context of globalization and post-industrialism in which they are also deeply implicated, a context marked by deepening social inequality and polarization.

Many of these approaches to the implications of ICTs for democratic citizenship treat the issue of *access* as central. To the extent that access to and skilled use of the Internet and other new ICTs has become central to economic, social, and political participation in information societies, so the argument goes, various digital divides must be narrowed in order to ensure that none are excluded (Castells 2001; Norris 2002; Wilhelm 2004). Many of these approaches are highly worthwhile; however, most tend to overlook the vital question of the politics behind the design of the very technologies and networks whose accessibility they seek to universalize.

Citizenship Code

This essay introduces another way of thinking about technological citizenship in the digital era, which I refer to as the problem of citizenship and *code*. By this I mean the ways in which, at the level of their technical design, the Internet, the World Wide Web and other new media structure and enable certain activities, conduct and forms of life on-line while they simultaneously constrain or neutralize others. My argument stems from the general proposition that embedded within all technological systems and artifacts in general are a variety of ethical, political and social norms. The design elements of such systems and artifacts can serve to hardwire certain forms of conduct, experience and social relations into our surroundings. In the context of digital technology and new media, the technical architecture of the Internet and the various software codes

and applications which run on it are analogous to legislative declarations and founding political documents which delimit the form, content and extent of citizen rights and obligations in a given polity. The degree to which Internet users can access information or navigate the web anonymously, for example, can be dictated at the level of code. As our daily lives are increasingly dependent upon, mediated through and enmeshed in the circuits of digital networks and computerized databases—to access information, government services and benefits, credit and insurance, health care, work, leisure and entertainment—we become subject to the terms and conditions of existence and action as laid down by code. Rose refers to this as "the cybernetics of control" which increasingly enwraps our daily existence (Rose 1999). But whereas the terms and conditions of political citizenship in liberal democratic states are, relatively speaking, subject to free, open and transparent deliberation and negotiation, the codes governing the citizen in the digital era are invisible and opaque, thanks to certain features of the technologies themselves, and to the proprietary nature of many of the codes increasingly mediating our lives.

Furthermore, I will argue, we have witnessed in recent years a more or less subtle adjustment of the terms and conditions of cybercitizenship at the level of code, according to which Internet users are being induced, habituated and, if necessary, compelled, to accept the norms of commercialized cyberspace, which include, *inter alia*, the commodification of personal information (and its accompanying erosion of privacy) and the aggressive expansion of intellectual property rights on-line (along with efforts to marginalize and criminalize widely practiced on-line activities such as music downloading). This renegotiation of the terms and conditions of cybercitizenship is taking place in the absence of democratic debate and discussion. It behooves us, therefore, as citizens of cyberspace, to read between the lines of code to decipher and respond critically to the constitutional fine print contained therein, before the terms and conditions of cybercitizenship they set forth become hardwired without our consent.

Part I: Citizenship and the Politics of Code

Technology as Legislation

The insight that technology and design embody certain values and goals, and that they can be used to regulate the conduct of individuals and populations for strategic ends can be traced back at least as far as nineteenth-century figures like Marx, Bentham and Haussman. Marx diagnosed the oppressive and alienating

effects of various technologies of capitalist industry, from the wage relation to mechanized factory production, while simultaneously recognizing the emancipatory potential of the socialization of labour under the factory roof. Bentham and Haussman, meanwhile, both incorporated corrective and strategic objectives into their respective designs for panoptic institutions and the streets of nineteenth-century Paris (precisely to neutralize the emancipatory pressures built up by capitalist technologies). In the twentieth century, Heidegger's critique of technology as an "enframing" of existence gave philosophical credence to the substantive view of technology as having effects that were far from neutral. Adorno, Ellul and Marcuse, among others, were the post-WWII heirs to the substantive tradition on the value-laden nature of technology. Perhaps it was Foucault's analysis of Bentham's *Panopticon*, however, which demonstrated so clearly to recent generations how technical design (the architectural achievement of hierarchical relations of visibility and invisibility between prisoner and warder, in this case) can embody strategic objectives and be used to achieve effects of power on those subject to it (Foucault 1977).

More recently, theorists of technology like Feenberg, Sclove and Winner portray technology and technical systems as unacknowledged *legislators* of human activity and social life which embody specific forms of power and authority (Feenberg 1991; Sclove 1995; Winner 1977; 1986). Here technological politics takes at least two forms. Specific technical innovations and designs can legislate social relations of power, as demonstrated by Robert Moses' efforts to hardwire racial and class segregation into the transportation grid of New York City by designing freeway underpasses to prevent public buses from accessing suburban (i.e. white) neighbourhoods (Winner 1986, 23). Feenberg also relates how what, in terms of its technical specifications, came to constitute a "steam boiler" in the nineteenth century was determined by shifting social judgments about worker safety and decades of political struggle, culminating in the development of uniform engineering codes of manufacture to reduce instances of "bursting boilers" (1995, 14). Sclove has also described how the introduction of private plumbing in a traditional Spanish village in the 1970s inadvertently dissolved key aspects of its traditional social life and culture, which hinged upon daily interactions at the village's communal fountain (3). Feenberg designates the embodiment of social and cultural values within the design features of artifacts as their "technical code" (1996, 78-83).

Secondly, whole technical systems such as industrialism, or energy and transportation grids, are linked to institutionalized patterns of power and

authority constitutive of social relations and daily life. The lethal properties and operational requirements of nuclear energy and armaments, for example, link their production to highly centralized, bureaucratic and secretive forms of administration hostile to democratic accountability (Winner 1986). More recently, Winner has shown, our increased dependence on highly complex technological infrastructures like the Internet and air transportation, coupled with their increased vulnerability to terrorist attack, has had chilling effects on civil and political rights in the name of "critical infrastructure protection" (2004).

The work of these authors demonstrates the significant degree to which the terms and conditions of modern citizenship are laid down by technical codes embodied in the technologies and technical systems in which our lives are enmeshed. The rights and obligations of citizenship are delimited as much, if not more, by these technical codes as they are by formal political declarations and codes of citizenship. As Feenberg declares:

> So far as decisions affecting our daily lives are concerned, political democracy is largely overshadowed by the enormous power wielded by the masters of technical systems: corporate and military leaders, and professional associations of groups such as physicians and engineers. They have far more to do with control over patterns of urban growth, the design of dwellings and transportation systems, the selection of innovations, our experience as employees, patients, and consumers, than all the governmental institutions of our society put together (1995, 3).

None of this is to suggest that all technology and technical systems are inevitably bound up with authoritarian rule and domination. Without underestimating the magnitude of the obstacles involved, all three authors hold out the possibility for a democratic reform of technology in the service of more humane goals, or what Feenberg calls "subversive rationalization" (1995). Technology is amenable to democratization; that is, it can respond to the assertion of new goals and values by incorporating new "technical codes" into its design and structure, as evidenced by the success of social movements over the last few decades in achieving a host of positive changes in areas ranging from workplace health and safety and environmental regulation, to nuclear power and biotechnology (20). A new, more humane form of technological society is possible as a result of collective mobilization and civic action on technological issues, that is, as citizens recognize and exercise the full rights and duties of technological citizenship.

In this paper I explore the nature and effects of information technology as legislation; that is, I illuminate some of the ways in which we are regulated and governed as citizens of cyberspace by the "technical code" embedded within various structures and features of the Internet and the World Wide Web. The technical coding of the Internet has ethico-political dimensions which impinge upon on-line citizenship by dictating who has access and under what kinds of conditions. After elaborating on the implications of code for on-line citizenship, the paper offers a number of concrete examples of the ways in which the design of Internet technologies serves to hardwire certain norms and practices of on-line citizenship. Finally, the paper considers the prospects for politicizing code and democratizing Internet design by examining the recent struggle between music copyright holders and downloaders, and the emergence of a self-conscious political movement around peer-to-peer networking and open-source software development.

The Politics of Code

If, as I suggest, the terms of on-line citizenship are increasingly hardwired into the digital networks of information and communication mediating everyday life, then we must interrogate the politics of the design of these very networks. Significant contributions to such an interrogation have been offered recently by Lessig (1999; 2001; 2004) and Galloway (2004), each of whom explores the politics of the technological infrastructure under-girding the Internet; how it structures and governs access to and conduct within cyberspace.

Lessig's basic argument, articulated in his first book, *Code: And Other Laws of Cyberspace*, is that the architecture of the Internet—i.e. software codes such as the Transmission Control Protocol/Internet Protocol (TCP/IP), which facilitates the transmission and reception data packets), and the Domain Name System (DNS), (which assigns and manages Internet names and addresses)—forms a constitution governing cyberspace and its inhabitants. "Codes," he writes, "constitute cyberspaces; spaces enable and disable individuals and groups. The selections about code are therefore in part a selection about who, what, and, most important, what *ways of life* will be enabled and disabled" (Lessig 1999, 66). In other words, in the digital world, Lessig writes, "code is law" (6). The framers of this digital constitution, if you will, are the engineers, designers and programmers of digital technologies. It is they, as much as it is conventional lawmakers and

regulators, who determine whether privacy is protected, anonymity allowed, and access guaranteed in cyberspace (60).

The original architecture of the Internet, Lessig argues, was designed to hardwire certain "hacker" values into the network itself. Through the development and proliferation of "open source" software codes like TCP/IP, UNIX, C++ and HTML, the Internet took the form of an open, distributed, and decentralized network that could be modified in an open and transparent fashion via negotiation and consensus-building among communities of experts and knowledgeable hobbyists. According to Lessig, these codes provided the Internet with its original "architecture of liberty" (30).

Galloway's recent book, *Protocol: How Control Exists After Decentralization*, highlights the ethico-political dimensions of the architecture of the Internet as well, substituting the term *protocol* for Lessig's *code*. Like code, *protocol* is constitutive of cyberspace and all that takes place within it. While, technically, *protocol* means little more than the "set of recommendations and rules that outline specific technical standards" for connecting to and transmitting information over the Internet (Galloway 2004, 6), *politically*, it is constitutive and enabling of connectivity and action on the network: "Protocol outlines the playing field for what can happen, and where." (167). The original protocols constitutive of the Internet embodied the hacker values of the loose-knit group of engineers, academics and computer hobbyists who devised, deliberated over and eventually agreed upon them (119-143). The values of decentralization, openness, transparency, consensus, flexibility, universal accessibility, anti-commercialism and anti-authoritarianism—values espoused by today's "open source" movement—were *designed into* the architecture of the Internet.[1]

Lessig and Galloway also describe the recent colonization of cyberspace by commercial, proprietary forms of code. Monopolistic proprietary software (e.g. Microsoft's Internet Explorer web browser), digital rights management (DRM) software (e.g. encryption and copy protection software embedded onto DVDs and CDs), and identification and authentication technologies (e.g. cookies, passwords, digital certificates, etc.) increasingly dominate the user's on-line experience. The transformation Lessig and Galloway describe is from an open, accessible and decentralized architecture designed to empower users to communicate and create, to a closed, opaque and proprietary one in which users are configured primarily as consumers, who are continuously incited to surrender both their credit card numbers and personal details in exchange for access to

information, cultural content and other electronic privileges. What distinguishes proprietary code is its development in closed, corporate-dominated circles, and the refusal of its commercial owners to reveal its source code and subject it to scrutiny and modification by the wider Internet public, as is done in the case of open source code.

Aiding and abetting the colonization of the Internet by proprietary code is the increasing involvement of governments in the politics of code, in the form of legislation designed to protect proprietary code and to stigmatize, and even criminalize, both the creation and use of certain kinds of code (e.g. viruses and peer-to-peer networks) which threaten commercial interests. In the U.S., the *Digital Millennium Copyright Act* (1998), or DMCA, prohibits, among other things, the reverse-engineering of proprietary software and criminalizes the development and distribution of software code designed to circumvent the encryption and copy-protection systems embedded into DVD movies and music CDs. Other examples include the *Computer Fraud and Abuse Act* (1986) targeting hackers and virus-writers, the *No Electronic Theft Act* (1997) which criminalized the copying and free distribution of copyrighted software, and a bill called the *Inducing Infringement of Copyrights Act* recently considered by the U.S. Congress, which proposes to make the operators of P2P networks liable for copyright infringement if copyrighted works are shared over their networks. In Europe, the EU Commission *Copyright Directive* (2002) and the Council of Europe *Convention on Cybercrime* (2001) contain many similar provisions. The World Intellectual Property Organization's (WIPO) copyright treaties of 1996 enjoin signatories to pass legislation to protect digital copyright and prohibit the development and distribution of DRM circumvention technologies.

Together, the colonization of cyberspace by proprietary code and various legislative initiatives designed to protect it, represent a major renegotiation of the terms and conditions of cybercitizenship as embodied in the design of the early Internet. Under the rule of proprietary code, the cybercitizen is being subtly reconfigured, *by design*, from an active subject of communication and creation into a passive consumer of on-line commercial products and entertainment. The following section offers concrete examples of the workings of proprietary code through a number of common technical design features of digital media, including web browser and cookie software, web portals and customization features, and digital rights management (DRM) technologies. Each of the technologies examined harbours implications for the terms of cybercitizenship and encodes particular ethico-political norms and values into the technical fabric

of cyberspace. The reconfiguration of the terms of cybercitizenship which these technologies effect is achieved via a gradual process in which new habits, expectations and practices on the part of web users are cultivated and/or inculcated through subtle mechanisms of inducement, coercion, and reward designed into the very experience of cyberspace. Such mechanisms subject users to what Luke calls the "hidden curriculum" of e-commerce, according to which web users are subtly configured into compliant consumers of digital media products and entertainment. The "hidden curriculum" of e-commerce technologies constitutes the new civic education for the citizens of an increasingly commercialized cyberspace (Luke 2004).

Part II: Digital Technology, E-Commerce and the "Hidden Curriculum" of the World Wide Web

Web Browsers and Cookies: Automating Choice

Web browser and cookie software have a significant impact on the experience of Internet users, mediating and filtering information they see and determining the amount of access, customization, and privacy they enjoy. The design features of popular web browser software products like Microsoft's Internet Explorer and AOL's Netscape Navigator subtly induce and coerce end-users into sacrificing on-line privacy in exchange for convenience and access to information According to Elmer, among others, surfers are *habituated* to surrendering personal information or submitting to surveillance as a result of the design of user interface software (Elmer 2002; Luke 2002). Web browser privacy controls can make retaining on-line anonymity more or less difficult, and have a tendency to steer users towards surrendering privacy. By setting factory default settings to automatically accept cookie files, and by burying cookie control functions deep within user preference settings and menus, (where they are unlikely to be accessed by the average user), browser software habituates surfers to comply with e-commerce's demand for personal information. Users who opt to maintain privacy are punished by being denied access to various sites, or they face increased inconvenience by having to continuously turn off cookie alerts.

Navigating the web, meanwhile, users are constantly confronted with web site features which demand personal information: passwords; log-ins; registrations, customization options etc. Users can elect not to provide this information, but in doing so they are penalized with restricted access and reduced convenience. Repeated experience of blocked or reduced access induces web surfers into

capitulating to the terms and conditions of cybercitizenship as dictated by e-commerce. Meanwhile, functions like Internet Explorer's "Autofill," which transmit personal information to complete standard information forms at the click of a button, routinize and normalize the surrender of information and privacy. Divulging such information has become what Elmer ironically calls the "automatic 'choice'" of web surfers, thanks to features built into the very design of browser software (Elmer 2002, 61). What follows from this routinized, induced publicity is the normalization of data capture and trace technologies which subject the Internet user to surveillance. Thus, as Luke points out, a "perpetual pedagogy of surveillance" is hardwired into the web, becoming "a hidden—and therefore uninterrogated—part of the process of learning to use the technologies of access" (Luke 2002, 74).

Such features are designed to support the commercial exploitation of the web, of course. E-commerce depends upon myriad opportunities for personal information to be surrendered and collected, usually in exchange for information and/or services like free e-mail or customized news headlines. The ideal on-line consumer is one who casually reveals her identity without undue regard for her privacy. Browser features like privacy/cookie settings and Autofill constitute what Luke calls the "hidden pedagogies of citizenship" for the world of e-commerce. "As they exchange personal information for dubious electronic privileges," Luke writes, "the lesson users are learning is one of compliance with the commercial imperatives of the corporate-controlled Net" (2002, 82).

Web Portals and Customization Tools: The Daily Me

Another aspect of web design which impinges on the nature of on-line citizenship is the proliferation of web portals through which users gain access to information and services customized to their specific needs and interests; a technology that Negroponte argues empowers users to radically personalize the flow of information entering their homes, resulting in what amounts to a "Daily Me" delivered to their electronic doorsteps (Negroponte 1995, 153). Web portals and customization tools enculturate users into certain kinds of habits, conduct and expectations that condition their use and experience of the web, with the potential for spillover into the off-line world. Luke (2002), Nakamura (2002), Patelis (2000) and Sunstein (2001) have all examined the hidden pedagogies of citizenship encoded into web portals. Firstly, reliance upon customizable web pages and portals (AOL, MSN, Yahoo, etc.) to filter and deliver information and news is relatively passive, since users are encouraged to assume a posture of

waiting for information to be brought to them on the basis of the preference/personalization settings and menu choices offered to them by the portal (Luke 2002, 66). Secondly, while marketed as neutral information conduits, portals and customization tools structure the content and customization options available to users through processes that are far from neutral. The web page convention of the "menu," for example, structures cyberspace as orderly and controlled, and defines for the user what kind of information is available and what the web can be used for (e.g. shopping, news, sports, horoscope, search, etc.). Decisions about the design, structure, content and customization options available on major web portals like AOL are far from neutral (Patelis 2000); more often than not they are dictated by commercial imperatives, such as maximizing web site "stickiness" and attracting "eyeballs" to web advertisements.

The customization features of web portals and on-line news alert services also encourage users to isolate themselves from events, information, experiences and voices which are of less interest or relevance to them (Sunstein 2001, 3-23). By filtering information and narrowing worldviews these same features work *on* the user's subjectivity as well (Nakamura 2002, 106). Portalization and customization facilitate the construction of on-line "fortified enclaves" of "intellectual isolation and insulation from difference" (Luke, 2002 76). The danger exists that the subtle pedagogies of portalization and customization will spill over into and affect civic life. The risks, as outlined by Luke, are that

> the willful segregation and/or self-imposed exile of individuals and groups within the online fortified enclave will become a grammar of action (or even democratic inaction) that reinforces segregation in the physical world...
>
> "If the digital citizen," he continues, "is constituted solely under the rubric of consumer empowerment, and this sense of empowerment is allied to a sense of entitlement and personal fulfillment only, then there is little room left for the negotiation of social difference. It is a slippery slope into intolerance from here" (77).

Digital Rights Management: Framing Cultural Citizenship through Code

Developments at the level of code are also having a dramatic impact on the terms and practices of cultural citizenship, generating sometimes acrimonious debate between producers and consumers of digital culture. In the last decade digital technologies have furnished millions with the ability to digitize and make copies of a wide range of cultural materials with no loss of fidelity in relation to the original, and which can be shared with others at the click of a mouse. As media and entertainment conglomerates sensed the danger posed by the democratization of the tools of cultural production, reproduction and distribution (what they refer to as digital "piracy") they began to invest in the development of software codes—digital rights management (DRM) technologies, in particular—designed to protect copyrighted works in digital format. Lessig's work has traced in detail the emergence and proliferation of the politics of code in the field of digital copyright in the U.S (1999; 2001; 2004). Along with aggressive legislative, public awareness and litigation strategies designed to reinforce the sanctity of copyright, new media industries in the U.S. in particular began to develop and embed DRM technology into their products in the 1990s. Under the leadership of the Motion Picture Association of America (MPAA), the film industry introduced its Content Scramble System (CSS) encryption software in 1994, which it encoded onto DVD movie releases thereafter. CSS was designed to prevent DVD movies from being played back on any device other than one licensed to decrypt CSS. In the late 1990s, meanwhile, a consortium of over 200 music recording and technology companies launched the Secure Digital Music Initiative (SDMI) which aimed to develop encryption code to protect copyrighted music in digital format. Today, tens of millions of music CDs have embedded copy protection software limiting the number of copies that can be made, the devices on which they can be played, and the ability of P2P users to "upload" music files onto the Internet. Federal legislation in the U.S., including the aforementioned DMCA, prohibits and criminalizes the production and use of software code designed to hack or circumvent DRM code, as we saw above.

Critics argue that the culture industries exaggerate the financial losses associated with digital "piracy," and that DRM technology and its accompanying legislative protections represent an attempt by these industries to exercise control over culture more thoroughly than ever before (Lessig 2004). Far from a defensive action, Lessig argues that DRM technology threatens to limit legitimate uses of copyrighted works far more strictly than they have been under previous regimes of "fair use" (116-173). Through code, the cultural industries are imposing new,

more restrictive terms and conditions of cultural citizenship upon the users and consumers of digital culture. Such attempts have not gone unopposed, however, by increasingly organized groups of hackers and consumers who, through their everyday practices of new media consumption and skilled use of technology, are articulating new cultural citizenship rights and obligations, as we shall see below.

The above examples suggest that the terms and conditions of access to cyberspace and the use of digital media are increasingly governed by commercial forms of codes embedded into the basic architecture and software applications of the Internet. These commercial forms of code have a number of properties and effects in common. Firstly, they structure the experience of cyberspace in such a way as to configure the user as a consumer, literally to *hardwire* commercial terms and conditions of citizenship into the electronic circuits of communication and consumption in contemporary capitalism. The colonization of cyberspace by commercial, proprietary code amounts to the declaration and enactment of a new constitution for cyberspace which lays down commercial terms and conditions of cyber-citizenship, including new rights (intellectual property) and obligations (compulsory visibility, identification, pay-per-view/play), and which also identifies and excludes non-citizens and outsiders (hackers, file-sharers, the unconnected). Secondly, proprietary code is designed through opaque processes of product-development and marketing by centralized, secretive corporations who conceal their source codes from the wider Internet public, this despite the fact that such codes have potentially profound implications for the production of users as subjects. Lastly, the production of new subjects and citizens of cyberspace through commercial code may spill over into and shape processes of subjectification in the off-line world as well, with troubling consequences for the cultivation of democratic citizens (Luke 2002; Sunstein 2001).

If, as the above suggests, the architecture and application programs which structure the experience of Internet users subject them to subtle and opaque disciplinary mechanisms which enculturate them into compliance with commercial objectives for cyberspace, then surely an adequate conception of technological citizenship for the digital era must include the politicization of code. Bringing the politics of code into the world of mainstream Internet users has been a challenge however. While software firms, the corporate media and U.S. legislators have for some time now demonstrated a sophisticated appreciation of the politics of code, the same cannot be said of average users and consumers of digital technology and new media. Until recently, the politics of code has been the province of hackers, cyber-activitists and their industry and

legislative adversaries. Notwithstanding a handful of high profile legal disputes, such as the Microsoft anti-trust case in the U.S., the politics of code has seldom hit the radar screens of average Internet users and citizens.

Among the obstacles to elevating the politics of code to popular consciousness are certain properties of new media technologies themselves. Much of the code regulating access to, conduct within, and experience of the Internet is largely invisible to users. A central feature of new media design, in fact, is that the source code for any particular application or program which structures an end-user's experience is hidden from them. "The job of computers and networks," according to Tim Berners-Lee, the inventor of HTML, "is to get out of the way, to not be seen" (quoted in Galloway 2004, 65). Code acts as its own "hiding machine," Galloway observes, "an apparatus to hide the apparatus" (75). HTML, IP addresses, and web browser software are exemplary of code's self-concealing character. HTML conceals the textual information which is ultimately responsible for the graphical web pages presented to surfers. Web browsers interpret, organize and filter HTML before presenting end-users with content while concealing their own editorial functioning.

In the last few years, however, the politics of code has assumed a more prominent place in key societal conflicts and debates over technology, law, and culture. The 2000-2001 Napster music downloading and file-sharing case is perhaps the most famous of these. In addition to introducing millions of new Internet users to the technologies of downloading and file-sharing over P2P networks, the high profile Napster dispute helped to foster the development of self-conscious social, cultural and political communities of P2P networkers who began to wake up to the possibilities as well as the risks of the politics of code. More recently, the Recording Industry Association of America (RIAA) filed more than 7,000 lawsuits against individual music downloaders and, with the help of other media industries and sympathetic legislators, is working to stigmatize, criminalize and sabotage popular peer-to-peer networks such as *KaZaa*, *Grokster*, and *BitTorrent*. For its part, I argue, the explosion in popularity of music downloading and P2P networking represents a form of resistance to proprietary code and an example of the *social appropriation* of the cultural and political possibilities of code. The final section of this paper examines the controversy over copyright, music downloading and peer-to-peer networking in light of the themes of citizenship and the politics of code outlined above. I argue that the politics of code lies at the centre of the current struggle between the music industry and the users of peer-to-peer networking and file-sharing

technology over the future of musical culture, and that the struggle pits two very different paradigms of digital citizenship against each other.

Part III: Digital Rights Management, Cultural Citizenship, and the Politics of P2P Networking

Code Wars: Digital Rights Management, Hacking and the Rise of P2P Networks

While the most visible signs of the current struggle over digital copyright manifest themselves in the legislatures and courts, its roots lie in developments at the level of code. Since the beginning of the 1990s, digital technologies have allowed Internet users to digitize and make copies of a wide range of cultural materials, and to make that material instantaneously available to others. This democratization of the tools of cultural production and distribution has been characterized by some as a shift to a more "participatory culture" (Jenkins 2004; Poster 2004). As we saw above, the cultural industries certainly sensed the potential threat posed by such as shift, and have responded with the introduction of DRM technologies to control the reproduction and distribution of copyrighted works, along with an aggressive legislative and 'public education' campaign to marginalize and stigmatize activities such as free music downloading as lying outside the bounds of responsible digital citizenship.

Opposition and resistance to the way in which code has increasingly been used by the cultural industries to legislate and control the use of digital media came from within the hacker community initially, with the release of software codes to circumvent DRM systems (Lessig 2001). DeCSS, for example, was created to disable the encryption system encoded onto DVDs, enabling them to be played on any machine (but not, it is worth mentioning, to be copied). A beta version of SDMI's encryption code for digital music recordings was publicly released in 2000, along with an invitation to the hacker community to try to "Hack SDMI." The SDMI code was cracked within weeks, wiping out two years of work and investment by the consortium. These and other examples suggest that, despite the subtle and hidden way in which software code governs the use of digital media, its authority to govern and regulate is not absolute.

With the appearance of free DRM circumvention programs in the late 1990s, media industries sought relief from legislatures and courts. In 1998, the U.S. Congress enacted the DMCA, which, by outlawing the development and distribution of DRM circumvention code, tipped the balance of power back in

favour of copyright holders. In 2002, for example, Hollywood filmmakers used the DMCA as the basis for launching lawsuits against the firm 321 Studios, the maker of DVD-copying software products, which circumvented the industry's CSS encryption code. Unable to sustain the costs of litigation, 321 Studios closed its doors in August of 2004 (Dean 2004). The DMCA was also the basis for the notorious July 2001 F.B.I. arrest of Dmitry Sklyarov, a Russian programmer, who was attending the Defcon hacker conference in Nevada. Sklyarov attended the conference to present software developed by his Russian employer, ElcomSoft, which enabled users to circumvent certain DRM features of *Adobe Acrobat e-Book* software. Sklyarov's arrest was widely reported as having been made at the behest of Adobe (Glasner 2002). Sklyarov was charged under the DMCA and held in U.S. custody for over six months and threatened with up to 25 years in prison before finally being released in exchange for testimony against his employer. The DMCA also provides the legal basis for the RIAA's legal campaign against music downloaders. In other words, when their own attempts to regulate and govern the use of digital media through technological means fail, the cultural industries will move quickly to recruit legislatures and courts to help ensure that countervailing technologies are stigmatized and criminalized.

Frustrated by these limits and empowered by a new generation of software tools like MP3 data compression and P2P networks, hackers and consumers have engaged in new rounds of resistance to DRM code and other attempts to control their habits and practices on-line. Practices such as downloading and file-sharing over P2P networks have become enormously widespread among American and other Internet users, and there is a high degree of acceptance of such practices as legitimate. By 2003 an estimated 35 million American adults had downloaded music from the Internet for free, while 26 million of these also shared files on-line (Pew Internet and American Life Project 2003). Two-thirds of this group said they did not care whether the files contained copyrighted works or not. At the time of writing, the world's most popular P2P networking software, *KaZaa*, had been downloaded almost 400 million times (KaZaa 2004). In light of such figures, the industry-led war on "piracy" can be read as a war on a set of popular, everyday practices and attitudes towards digital media consumption embraced by hundreds of millions of Internet users worldwide, practices which themselves speak to a popular urge to appropriate new media in ways which challenge the traditional commercial model of producing, distributing and consuming cultural material.

KaZaa Nation: Culture and Community in the Era of P2P Networks

While dismissed by industry as a malignant form of disregard for ownership, intellectual property and the value of music, critical media scholars have read the popular embrace of downloading and P2P networking quite differently—as prefiguring new forms of cultural citizenship and community on-line. Numerous scholars have drawn attention to the broader cultural and social significance of P2P networks, music downloading, and file-sharing. Viewed in historical context, they can be seen as recent iterations of the "participatory turn" in culture enabled by new technologies which blur old distinctions between producers and consumers of culture (Jenkins 1992; Uricchio 2002, 5-6; Ebare, 2004). Digital technologies have helped to diffuse, decentralize and de-hierarchize the means of cultural production, distribution and consumption by, for example, increasing access to studio-quality recording technology or enabling downloaders to assemble their own customized MP3 "playlists" of favourite artists and songs. From this perspective, downloading and file-sharing (of images, movies, text and software, as well as music) constitute the typical activities and practices of an emerging "digital culture" (Jenkins 2004; Poster 2004).

Music downloading and file-sharing have also been the focus of sociological studies of on-line music communities *qua* community. On-line community is now a well-established if somewhat contested concept in the social sciences (Smith & Kollock 1999). Cultural significance is to be found in on-line music-sharing communities as virtual places where music fans gather, produce and exchange cultural goods, communicate with and educate one another, and express and affirm their identities (Ebare 2004; Poblocki 2001; Uricchio 2002). Virtual communities formed around shared interests and the free exchange of information, ideas and cultural content—from news blogs and fan sites to academic listservs and free software communities—have also been characterized as participating in on-line "gift economies" outside the cash nexus of commodified social relationships (Barbrook 1998; Stalder 1999). Viewed in such light, downloading and file-sharing constitute the expression and enactment of a more participatory form of cultural citizenship: one in which musical culture is produced and enjoyed in a collaborative, decentralized and dehierarchized fashion "outside the framework of commodification" (Uricchio 2002, 19).

Copyright, Music Downloading and the (not so) Hidden Curriculum of Digital Citizenship

Predictably, the explosive popularity of music downloading and file-sharing produced alarm within the cultural industries, particularly among executives in the music industry. At stake, according to the industry, are the rights of artists and copyright holders to just compensation for their creative works, and the very survival of music itself. According to figures from the International Federation of the Phonographic Industry (IFPI), retail sales of CD and cassette sound recordings in mature markets like the U.S. have decreased by almost 30%, representing losses in the billions of dollars (IFPI 2004). The industry attributes these losses almost entirely to the explosive growth of music downloading and file-sharing.[2] Sensing that we are on the cusp of a major restructuring of the terms of cultural citizenship, the recording industry and its allies in film, publishing, proprietary software and other forms of intellectual property are attempting via an aggressive politics of code to ensure that the potential of P2P networks goes unrealized. Since 2000, the music industry has pursued a strategy designed to steer and coerce Internet users into practices and habits of new media consumption more compatible with their own agenda and financial interests, as well as the broader capitalist model of cultural citizenship. This strategy includes technological, "public awareness," legal and legislative components, all of which are deeply implicated in a reactionary politics of code. Together, the components of the industry strategy articulate a distinct vision and pedagogy of good cultural citizenship in the digital age, one based on the centrality of the commodity form and the social relations wrapped up within it. This industry vision of cultural citizenship simultaneously disparages and undermines competing paradigms of cultural citizenship which, as I argued above, are prefigured in practices like P2P networking and music downloading and file-sharing. Let us take a closer look at the industry strategy.

Prior to launching its more aggressive campaign of lawsuits against individual downloaders in 2003, the recording industry in the U.S., led by the RIAA, initiated a number of programs designed to dampen Internet users' enthusiasm for downloading. Firstly, as noted above, the industry took technological measures to prevent or reduce the incidence of CD copying and uploading by embedding copy protection software in its products. In addition, the RIAA and its member companies have also used more clandestine technological measures, including electronic surveillance of P2P users and the sabotaging of P2P networks, in their battle with downloaders and file-sharers. The RIAA and

various member companies have used the services of Internet security firms, like New York-based MediaSentry, to monitor users of P2P networks and to identify the most enthusiastic file-sharers. MediaSentry advertises a number of "anti-piracy solutions" on its web site. *MediaSentry* software patrols over 25 popular P2P networks for copyright infringements and captures information on users such as usernames and IP addresses, while *MediaDecoy* attempts to deter file-sharing and downloading by, in the company's own words, "overwhelming file trading communities with non-working versions of your copyrighted material" (MediaSentry 2004). It is also worth noting that such Internet vigilantism has not only been exempt from the U.S. *Computer Fraud and Abuse Act* (under which the propagators of other forms of illicit code, such as hackers, are prosecuted), but is currently being considered for legislative endorsement under a federal bill that would limit the liability of copyright holders for the damages done to P2P networks in their efforts to protect their copyrighted works. In other words, in the defense of intellectual property, *bad code* promotes good cultural citizenship.

The cultural industries threatened by downloading and file-sharing have also launched major public awareness campaigns to "educate" consumers on the issues of copyright, file-sharing and the alleged risks of participating in P2P networks. The recording industry in the U.S. launched simultaneous print, TV, web and point-of-sale advertising campaigns warning music downloaders of potential copyright infringement, as well as other risks such as vulnerability to hacking and viruses, as a result of participating in P2P networks. In 2003, meanwhile, in cooperation with the pro-free enterprise student club Junior Achievement, the MPAA succeeded in introducing a "Digital Citizenship Lesson Plan" into the U.S. school curriculum which preaches about the legal as well as moral hazards of file-sharing. The MPAA curriculum package reached upwards of 900,000 students in 36,000 classrooms that year alone (MPAA 2003). Throughout such material the practices of downloading and file-sharing are stigmatized and delegitimized by the use of terms like "piracy," "theft," and "trafficking."

When the music industry's technological and educational efforts failed to make a sufficient dent in the growth of downloading and file-sharing, it adopted the more aggressive and direct strategy of filing lawsuits against individual music downloaders and uploaders. Since April 2003, RIAA has filed suits against over 7,000 individuals, ranging from 12 year-olds to college students and grandparents, and has settled out of court with thousands of them, usually for sums in the thousands of dollars.

The recent lawsuits by RIAA represent a significant shift in industry tactics, since they target individual consumers of digital music, where previous industry efforts had been focused primarily on file-sharing networks like Napster and KaZaa. Targeting individual consumers in this way carries a certain degree of risk, since it may alienate the wider music audience. But the industry portrays itself as fighting for survival, for the sustainability of its own business model for the commercial music industry. The future of that model depends, among other things, on cultivating disciplined *consumers* of digital music habituated to paying for music on and off-line. The industry's effort to cultivate willing consumers of commodified music involves a multifaceted program designed to adjust the habits, practices and mindset of the millions of Internet users who currently download and share music files for free. It is within the context of this broader effort to cultivate and discipline music consumers that the lawsuits by RIAA are best understood, an effort involving measures of both persuasion and coercion. Whether RIAA succeeds in recouping the alleged losses of its members is really beside the point. The clear intent of the lawsuits is to discourage the use of file-sharing software and to discipline consumers into abiding by RIAA's expansive interpretation of its members' rights and the commercial model of cultural citizenship to which they are bound.

The RIAA lawsuits appear to be having some effect. The percentage of Internet users in the U.S. downloading music dropped by half, from 29 to 14 percent, between April 2003 and January 2004. The percentage of those who shared files of any kind, music or otherwise, declined from 28 to 20 in the same period. At the same time, the percentage of Internet users running P2P applications like KaZaa and Grokster on their computers dropped anywhere between 15 and 59 percent depending on the service used (Pew Internet and American Life Project 2004). In addition, more and more consumers are turning to paid download sites. In the U.S., sites like Apple iTunes are visited by millions of users every month. Apple iTunes reached the 50 million download mark in March 2004 (IFPI 2004).

To be sure, however, a new generation of hackers and tech-savvy new media consumers, many of whom have become involved in the growing, self-conscious P2P advocacy movement, will continue to pursue a progressive politics of code armed with new software tools, including a new generation of free downloadable P2P software such as *Blubster*, *e-Donkey* and *BitTorrent*. Indeed, one of the virtues of such struggles is that they have raised public awareness of the politics of code and have renewed interest in open source code, free software and so-

called "copyleft" as *political* responses to corporate control of new media, and have furnished consumers and hacktivists with new means with which to pressure for media reform.

Whatever the outcome of this most recent legal skirmish between the music industry and the defendants in the downloading cases, the legal/technological/ideological and legislative battle over downloading and file-sharing is an important one. When one considers the extent of the practice of downloading and file-sharing by Internet users, the potential cultural importance of these new forms of consumption and distribution, and the aggressive response to them on the part of media companies and legislators, one can discern the makings of a major societal and cultural struggle over the future framework for producing, distributing and consuming culture. These legal, technological and cultural struggles pit two conflicting models of cultural citizenship against one another. Against the cultural industries' model of consumer citizenship as compliance with copyright stand consumers' claims to a more participatory form of cultural citizenship, in which control of musical production and distribution is wrested from the clutches of industry. Above all, the struggle over digital copyright has exposed the politics of code and demonstrated the ways in which the terms and daily enactment of citizenship can be hardwired into the digital environments in which we increasingly operate. This calls for a new progressive politics of code which is emerging as we speak, and for critical reflection on its potentialities and limitations.

Open Source: Prefiguring a Democratic Politics of Code?

Let me conclude by anticipating and addressing a question begged by the analysis and argument present thus far: if P2P networking and music downloading/file-sharing prefigure new models of cultural citizenship on-line, what form would a progressive, non-proprietary politics of code for cybercitizneship in general look like? My tentative reply is that it might look something like the recently resurgent hacker-inspired open source software movement oriented around open source codes like Linux, GNU, Apache and HTML, and led by groups such as FLOSS and the Free Software Foundation. The main principles of open source code development today consist of the following: collaborative and inclusive design; openness and transparency of source code; openness of the code to ongoing modification, negotiation and refinement; universal access to software at little or no cost; non-restrictive licensing to encourage use and improvement of the code (Jesiek 2003; Moody

2001). Open source coding as a social movement has emerged and grown into a self-conscious social movement since the late 1990s in direct response to the colonization of the Internet by a few monopolistic software firms, most notably Microsoft. While often viewed as obscure, open source code has begun to make a mark on cyberspace. The Apache HTTP open source web server code is now run on roughly 65 percent of all web sites, and the open source Linux operating system has increasingly become the system of choice in the public sector and for a variety of otherwise proprietary systems and devices (Jesiek 2003). MySQL is a free, open source analog of the proprietary database software Oracle. The open source Mozilla web browser and email software is increasingly popular in the wake of revelations about the security and privacy shortcomings of Microsoft's Internet Explorer. Finally, HTML, the basic code on which the web operates, was publicly released as an open source project by its inventor, Berners-Lee, in 1993.

While the open source movement emerged in the late nineties, its predecessors in the free software and hacker movements have been around for two decades. In fact, many early hackers, as well as the electrical engineers and computers scientists involved in the RFC process out of which the original Internet protocols emerged were committed for all intents and purposes to the ethic of open source software development. As recounted by both Lessig and Galloway, the open source process by which the early Internet protocols were written was informed by basic beliefs espoused by lead hackers, such as Eric Raymond, that "information-sharing is a powerful, positive good, and that it is an ethical duty of hackers to share their expertise by writing open-source code and facilitating access to information and to computing resources" (Jesiek 2003).

The ethics and practice of open source software design offer an alternative politics of code to that offered by proprietary software and harbour a broader vision of a more transparent, open and inclusive Internet architecture more consistent with the norms and values of democratic citizenship. Firstly, in both procedure and substance the practice of open source code articulates and hardwires certain constitutional rights (access to source code and its subsequent development) and obligations (transparent, inclusive, and flexible design processes) into the coding of the Internet and new media. Secondly, in so far as open source code offers a counter-image of digital citizenship to that embodied in the opaque workings of proprietary code (controlled access, secrecy of source code, compulsory publicity for users, etc.), it constitutes a *hack* of cybercitizenship as it has been configured by Microsoft, AOL and others. Open source affords the possibility of users once again openly collaborating to assess,

revise and improve the technical codes that increasingly govern their lives, according to their needs, as they see fit. As Jesiek writes:

> When key software technologies are developed in a closed-source, corporate environment, the negotiating power of marginalized social groups and users is…diminished. Various forms of resistance may appear…but these reactive efforts are constrained by the technical codes built into the technologies by those in power. In the open source world, actors have one more degree of freedom, allowing for the proactive shaping and modification of technologies, both in design and use (2003).

As such, open source fits with Galloway's injunction that we must avoid futile attempts to refuse code and, rather, "direct these protocological technologies, whose distributed structure is empowering indeed, toward what Hans Magnus Enzenberger calls an 'emancipated media' created by active social actors rather than passive users." (Galloway 2004, 16).

The image of technological citizenship that I argue is captured in the open source software movement is far from perfect. As a movement, it is prone to a certain technical elitism which produces forms of knowledge and discourse among members that average users often do not understand. As Jordan and Taylor argue, "[t]he purity of [open source's] commitment to elegant software hacks often isolate[s] it from vast areas of society which could never hope to use or understand the works of its adherents" (Jordan and Taylor 16). And yet, despite its flaws, open source prefigures a promising new politics of code and offers us a counterimage to the model of on-line citizenship embodied in the technological infrastructure of e-commerce.

Conclusion

To the extent that Internet users are subject to law-like codes regulating, enabling and constraining on-line behaviour and access to information, our understanding of technological citizenship in the digital era must transcend preoccupations with the digital divide, electronic voting and the like, to interrogate the terms and conditions of digitally encoded citizenship. We must examine more fully the socio-technical means by which Internet users become citizens of cyberspace via subtle processes of enculturation, inducement and coercion, as well as how they resist and rearticulate, through their daily practices and social appropriation of the technology, the terms and conditions of citizenship imposed by its current

configuration. What are the possibilities of the politics of code for the democratic reinvention of the cyberspace? What are the limits and dangers? Beginning to understand the imposition of a given Internet architecture, along with the ways in which users both acquiesce to and resist it helps us move beyond the limits of current thinking about the citizenship in the Internet era and to open up new branches of inquiry and critical reflection.

References

Ball, Kirstie & Frank Webster (eds.). 2003. *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press.

Barbrook, R. 1998. "The High-Tech Gift Economy." *First Monday* 3(12): December (at http://www.firstmonday.org/issues/issue3_12/barbrook/).

Barney, Darin. 1996. "Push-button Populism: The Reform Party and the Real World of Teledemocracy." *Canadian Journal of Communication* 21(3): 381-413.

_____. 2000. *Prometheus Wired: The Hope for Democracy in the Age of Network Technology*. Vancouver: UBC Press.

Borsook, Paulina. 2000. *Cyberselfish: A Critical Romp Through the Terribly Libertarian Culture of High-Tech*. Washington DC: Public Affairs.

Castells, Manuel. 1989. *The Informational City: Information Technology, Economic Restructuring and the Urban-Regional Process*. London: Blackwell.

_____. 2001. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford Univ. Press.

Dean, Katie. 2004. "321 Studios Shuts Its Doors." *Wired*. (3 August) (at http://www.wired.com/news/digiwood/0,1412,64453,00.html).

Diebert, Ron. 2003. "Civil Society Networks in an e-Connected World." In *The e-Connected World: Risks and Opportunities*, ed. Stephen Coleman. Montreal: McGill-Queen's Univ. Press, 107-122.

Ebare, Sean. 2004. "Digital music and subculture: Sharing files, sharing styles." *First Monday* 9(2): February (at http://firstmonday.org/issues/issue9_2/ebare/index.html).

Elmer, Greg. 2002. "The Case of Web Browser Cookies: Enabling/Disabling Convenience and Relevance on the Web." In *Critical Perspectives on the Internet*, ed. Greg Elmer. Lanham, MD: Rowman and Littlefield, 49-62.

Feenberg, Andrew. 1991. *Critical Theory of Technology*. Oxford: Oxford Univ. Press.

_____. 1995. "Subversive Rationalization: Technology, Power and Democracy." In *Technology and the Politics of Knowledge*, ed. Andrew Feenberg and Alastair Hannay. Bloomington: Indiana Univ. Press, 3-20.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. Trans. Alan Sheridan. New York: Pantheon.

Galloway, Alexander R. 2004. *Protocol: How Control Exists after Decentralization*. Cambridge, MA: MIT Press.

Gandy, Oscar H. Jr. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder: Westview Press.

Hill, Kevin A. & John E. Hughes. 1998. *Cyberpolitics: Citizen Activism in the Age of the Internet.* Lanham, MD: Rowman & Littlefield.

Glasner, Joanna. 2002. "Jury Finds ElcomSoft Not Guilty." *Wired*. (17 December), at http://www.wired.com/news/business/0,1367,56894,00.html.

IFPI. 2004. "Global music sales fall by 7.6% in 2003—some positive signs in 2004." (7 April), at http://www.ifpi.org/site-content/statistics/worldsales.html.

Introna, Lucas, and Helen Nissenbaum. 2000. "The Public Good Vision of the Internet and the Politics of Search Engines." In *Preferred Placement: Knowledge Politics on the Web*, ed. Richard Rogers. Maastricht: Jan van Eyck Editions, 25-47.

Jenkins, Henry. 1992. *Textual Poachers: Television Fans and Participatory Culture*. New York: Routledge.

Jenkins, H. 2004. "The Cultural Logic of Media Convergence." *International Journal of Cultural Studies* 7(1): 33-43.

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

KaZaa. 2005. at http://www.kazaa.com/us/index.htm.

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

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

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

Luke, Robert. 2002. "Habit@online: Web Portals as Purchasing Ideology." *Topia: A Canadian Journal of Cultural Studies* 8: (Fall), 61-89.

_____. 2004. "The Hidden Curriculum of Web Portals: Shaping Participation in Online Networks." Ph.D. diss., University of Toronto.

Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

McChesney, Robert W. 1999. *Rich Media, Poor Democracy: Communication Politics in Dubious Times.* New York: The New Press.

MediaSentry. 2004. "Solutions Overview." at http://www.mediasentry.com/services/.

Mitchell, William J. 1995. *City of Bits: Space, Place and the Infobahn*. Cambridge MA: MIT Press.

Mosco, Vincent and Dan Schiller (eds.). 2001. *Continental Order?: Integrating North America for Cybercapitalism*. Lanham, MD: Rowman and Littlefield.

Motion Picture Association of America (MPAA). 2003. "Film/TV Industry Launches Public Service Announcement as Part of Nationwide Awareness Campaign on the Impact of Digital Piracy." Press Release, 22 July, at http://www.mpaa.org/MPAAPress/2003/2003_07_22a.pdf.

MTV News. 2003. "Digital Decoys Are Making Frustrated Pirates Say 'Arrr'." (3 November) at http://www.mtv.com/news/articles/1470464/20030310/linkin_park.jhtml?headlines.

Murdock, Graham and Peter Golding. 2001. "Digital Possibilities, Market Realities: The Contradictions of Communications Convergence." In *Socialist Register 2002: A World of Contradictions*, eds. Leo Panitch and Colin Leys. Halifax: Fernwood, 111-129.

Nakamura, Lisa. 2002. *Cybertypes: Race, Ethnicity, and Identity on the Internet*. New York: Routledge.

Norris, Pippa. 2002. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge: Cambridge Univ. Press.

Oberholzer, Felix and Koleman Strumpf. 2004. "The Effect of File Sharing on Record Sales: An Empirical Analysis." March, at http://www.unc.edu/~cigar/papers/FileSharing_March2004.pdf.

Patelis, Korinna. 2000. "E-Mediation by America Online." In *Preferred Placement: Knowledge Politics on the Web*, ed. Richard Rogers. Maastricht: Jan van Eyck Editions, 49-63.

Pew Internet and American Life Project. 2003. "Music Downloading, File-sharing and Copyright." Data Memo, July (at http://www.pewInternet.org/pdfs/PIP_Copyright_Memo.pdf).

_____. 2004. "The impact of recording industry suits against music file-swappers." Data Memo, January (at http://www.pewInternet.org/pdfs/PIP_File_Swapping_Memo_0104.pdf).

Poblocki, Kacper. 2001. The Napster Network Community. *First Monday* 6(11): November (at http://firstmonday.org/issues/issue6_11/poblocki/index.html).

Poster, Mark. 1995. "CyberDemocracy: Internet and the Public Sphere." (at http://www.hnet.uci.edu/mposter/writings/democ.html).

_____. 2004. Consumption and digital commodities in the Everyday. *Cultural Studies* 18 (2-3): March/May, 409-423.

Recording Industry Association of America (RIAA). 2003. "Issues: Anti-Piracy." (at http://www.riaa.com/issues/piracy/default.asp).

Robins, Kevin and Frank Webster. 1999. *Times of the Technoculture: From the Information Society to the Virtual Life*. London: Routledge.

Rose, Nicolas. 1999. *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge Univ. Press.

Saco, Diana. 2002. *Cybering Democracy: Public Space and the Internet.* Minneapolis: Univ. of Minneapolis Press.

Sassen, Saskia. 1998. *Globalization and Its Discontents: Essays on the New Mobility of People and Money*. New York: The New Press.

Schiller, Herbert. 1996. *Information Inequality: The Deepening Social Crisis in America.* New York: Routledge.

Sclove, Richard. 1995. *Democracy and Technology*. New York: Guilford Press.

Smith, Marc A. and Peter Kollock (eds.). 1999. *Communities in Cyberspace*. London: Routledge.

Stalder, F. 1999. "Beyond Portals and Gifts: Towards a Bottom-Up Net-Economy." *First Monday* 4(1): January (at http://www.firstmonday.org/issues/issue4_1/stalder/).

Sunstein, Cass. 2001. *Republic.com*. Princeton NJ: Princeton Univ. Press.

Uricchio, William. 2002. "Cultural Citizenship in the Age of P2P Networks." Paper presented at Modinet: Inaugural Conference, 6 September, University of Copenhagen, Copenhagen, Denmark (at http://www.hum.ku.dk/modinet/.)

Wilhelm, Anthony. 2000. *Democracy in the Digital Age.* London: Routledge.

_____. 2004. *Digital Nation: Toward an Inclusive Information Society.* Cambridge MA: MIT Press.

Winner, Langdon. 1977. *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought.* Cambridge MA: MIT Press.

_____. 1986. *The Whale and the Reactor: A Search for Limits in an Age of High Technology.* Chicago: Univ. of Chicago Press.

_____. 2004. "Trust and Terror: The Vulnerability of Complex Socio-technical Systems." *Science as Culture* 13(2): June, 155-172.

---

[1] Not everyone would agree with this admittedly rather sanguine characterization of hacker values. Crude forms of sexism and libertarianism are also well-represented in the culture of computing and the Internet. Cf. Borsook 2000.

[2] A number of recent studies have cast doubt on the link between downloading, file-sharing and declining CD sales. General business conditions, such as a decline in overall consumer spending, and strategic failures and miscues on the part of industry itself, have also been blamed. Cf. Oberholzer et al. 2004.