Surveillance and Democracy in the Digital Enclosure

Jennifer R. Whitson
PhD Student
Department of Sociology and Anthropology
7th Floor, Loeb Building
Carleton University
1125 Colonel By Drive
Ottawa, Ontario, Canada K1S 5B6
jwhitson@connect.carleton.ca

[Draft: Please do not quote without permission from the author]

Abstract:
The absence of elected governments in cyberspace, on one hand, has increased freedom of expression and creativity, and allowed the formation of online communities that are governed from the bottom-up. On the other hand, the lack of a democratic process also allows corporations to step in as *de facto* governments, and privatize increasing areas of online space (e.g. Google, MSN, Yahoo, AOL, Facebook). Once hailed as a place where users could escape hierarchical control and the tyrannies of government, the Internet is now subject to an enclosure movement, wherein public "land" is being privatized, and citizen's creative labour is appropriated to profit the corporations that administer these places. The extent of surveillance in these spaces may surpass any in the terrestrial world, yet the façade of democracy –communities labouring together as equals to create idealized spaces—is used to attract more citizens. The gap left by elected governments, especially nation-state governments, allows corporations to conquer online spaces. The forms of participation, creativity, and empowerment open to users are harnessed to corporate drives for efficiency and profitability. Rather than working to correct power asymmetries in society, as predicted by early decentralized models of the Internet, the Internet contributes to ever-increasing levels of surveillance, concentrates power in the hands of a few, and erodes transparency and openness. While the Internet is seen as democracy-promoting in terms of how it affords potentials for creativity and political organization from below, it is increasingly important to examine how new media is appropriated for corporate ends, and how this alters the democratic potential of the Internet. The history of Second Life (SL), an online virtual world with over 14 million 'residents', provides a paradigmatic example of the digital enclosure movement. It is used throughout this paper to highlight the interplay between privatization, user-created content, the promise of online democratic spaces, and surveillance.

Keywords: surveillance, democracy, cyberspace, control, Second Life

Jennifer R. Whitson is a Sociology PhD student at Carleton University. She holds a Canada Graduate Scholarship and was co-editor of the 2005 special double volume of the journal Surveillance and Society on 'Doing Surveillance Studies'. Her current research interests include digital identity management, governance in online domains, identity theft, and software development processes. Her most recent article on identity theft, co-authored with Kevin Haggerty, appeared in the journal *Economy & Society* in November 2008.

Surveillance and Democracy in the Digital Enclosure

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> *Excerpt from John Perry Barlow's Declaration of the Independence of Cyberspace*(Barlow 1996)

The absence of elected governments in cyberspace, on one hand, has increased freedom of expression and creativity, and allowed the formation of online communities that are governed from the bottom-up. On the other hand, the lack of a democratic process also allows corporations to step in as *de facto* governments, and privatize increasing areas of online space (e.g. Google, MSN, Yahoo, AOL, Facebook). Once hailed as a place where users could escape hierarchical control and the tyrannies of government, the Internet is now subject to an enclosure movement, wherein public "land" is being privatized, and citizen's creative labour is appropriated to profit the corporations that administer these places. The extent of surveillance in these spaces may surpass any in the terrestrial world, yet the façade of democracy –communities labouring together as equals to create idealized spaces—is used to attract more citizens. It is a cruel joke that the unregulated spaces idealized by techno-libertarians of the 90's have now become sites of surveillance and control. The gap left by elected governments, especially nation-state governments, allows corporations to conquer online spaces. Unlike elected governments, these

corporations are not accountable to their "citizens", cannot be disposed of, and their practices and internal workings are nearly opaque.

The history of Second Life (SL), an online virtual world with over 14 million "residents", provides a paradigmatic example of the enclosure movement. It is used throughout this paper to highlight the interplay between privatization, the promise of online democratic spaces, and surveillance. While these kinds of enclosure movements are taking space in many kinds of online spaces, I draw examples from a virtual world to further demonstrate how avatars, the characters that users choose to represent them in these worlds, facilitate surveillance and challenge traditional notions of online anonymity. While SL will likely be replaced by more technologically advanced virtual worlds, as an example, it has much to say about the corporate incursion into online spaces, the expansion of asymmetrical surveillance practices and power relations, and the resultant transformation of spaces originally created with the most democratic ideals. Second Life is just one instance where the hype of community participation and co-production of economic wealth in online spaces is under-pinned by increasing corporatization, surveillance, and control.

What Went Before: The Myth of the Commons

Barlow's famous Declaration of the Independence of Cyberspace evokes the picture of an online intellectual commons free from government control. This picture is reinforced by technical descriptions of how the Internet works. Originally created by DARPA (the United States Defense Advanced Research Department), the Internet was designed to ensure quick, unhindered communication in the event of nuclear attack. It is a distributed

network that has no central site of control, and can be rudimentarily envisioned as a massive web, with each computer on the web linked to and able to communicate with any other computer. Consequently, if one node of the network is inoperable, the message automatically diverts to an alternate route and communication continues. Extrapolating from this model and the "protocol" (Galloway 2004) associated with it, the Internet is seen by many, including media scholar Mark Poster as a place explicitly designed "with no attention at all to questions of who is authorized to speak, when, to whom, and what may be said on these occasions (Poster 2004).

The architecture of the Internet allows for ease of information access, facilitates communication, and promotes the formation of community over long distances (Rheingold 2000). This architecture, it is claimed, levels terrestrial communication hierarchies because the identity of the information sender has no effect on the priority and speed of the message, thus ensuring equality regardless of the social power or economic status of the sender. Accordingly, the Internet is seen by many as a revolutionary medium that gives equal voice to all citizens, especially in contrast to pre-existing media forms (e.g. television, newspaper, and radio networks), that are commonly characterized as top-down one-way communication channels controlled by media elites. The technical capabilities of the Internet are held as proof that the Internet is inherently threatening to centralized, hierarchical power relations (Andrejevic 2007; Galloway 2004).

By definition, convivial technologies are transparent, accessible, and flexible in terms of being easy to use and modify (Monahan 2008). While they are predominately small-scale, the decentralized network of the Internet encourages participation, diverse modes of expression and power equalization—all of which characterize convivial

technologies. For example, the opportunity to make oneself heard through webpages, blogs, and video postings is believed to foster democratic engagement and empower internet users to actively participate in online environments.

Second Life exemplifies the convivial in its proclamation that it is "imagined, created, and owned by its residents" (Linden Lab 2006). Second Life is largely the vision of Philip Rosedale, founder of Linden Lab. It was originally designed as an online 3D environment devoted to task-based games and socialization, but during an early meeting with investors, Rosedale noticed that the participants were particularly responsive to the collaborative, creative potential of SL. The most popular application in SL was the 3D modelling tool that allowed users to create avatars, buildings, clothing, and animations in-world. As a result, the initial gaming focus of SL was shifted to a more user-created, community-driven experience that was partly inspired by Rosedale's experiences at the radical Burning Man festival (Au 2008a).

Launched in June 2003, the SL platform started as a blank slate where the first visitors could build any content they chose. However, Linden Lab discovered that without incentive to create, SL content evolved slowly, a problem given that novel content was necessary to attract new "residents" (the term preferred by Linden Lab and SL users alike). On the verge of financial ruin, Linden Lab consulted with prominent technology activist and scholar, Lawrence Lessig, and decreed that inhabitants could own and resell virtual land, own intellectual property and have the ability to claim copyright on their designs. The mixture of a community-driven experience, creative freedom, and the ability to profit from selling one's designs in-world has proved to be a successful combination. SL has grown phenomenally—from just over 1000 residents in November

2003, to 180,000 in April 2006, to over 14 million residents today. SL is particularly convivial as sections of its underlying code are open-source, meaning that residents can access the inner workings of the SL platform, determine how it works and make modifications and improvements. Yet, when the daily operations of SL are closely examined, many elements of SL are at odds with this initial assessment of its convivial nature. This finding extends to the Internet more generally, as well.

The Digital Enclosure Movement and the Rise of the Surveillant Society

The myth of the intellectual commons, where ideas are freely circulated and everyone is equal, fails to hold up to scrutiny when we move from abstract diagrams to concrete examples. While at one point the Internet *may* have fit the description of a convivial technology, the increasing privatization of online spaces by large corporations results in asymmetries in the power relations between corporations and individual users, asymmetries that belie the democratic ideals that the internet is assumed to foster. On top of decentralized network model of the Internet lies another model wherein the creation of privatized spaces—digital enclosures—allows corporations to control whom is authorized to speak, when and to whom. Moreover, these spaces are characterized by asymmetries in visibility, whereby corporations have significant surveillance powers while their own actions are increasingly opaque.

Communications scholar Mark Andrejevic describes a digital enclosure as "...the creation of an interactive realm wherein every action and transaction generates information about itself (Andrejevic 2007: 2). For Andrejevic, the Internet as a whole provides a paradigmatic example of a digital enclosure—one in which every virtual

"move" has the potential to leave a digital trace or record of itself. These digital traces are assembled into informational profiles of users, which can be used to improve the user experience, subtly shape user's desires and behaviours, or be profitably sold to other corporations (Gandy 1993). The digital enclosure concentrates an unprecedented amount of control over digital information in the hands of a few via asymmetrical surveillance practices.

The term "digital enclosure" consciously evokes the land enclosure movement of the eighteenth and nineteenth centuries, where public farmland in England and Wales was appropriated for private benefit. With the historical land enclosure movement, the appropriation of public land allowed private landowners to set the conditions of its use. It resulted in the formation of distinct classes because it separated those who owned and administered the land from those who had to sell their labour for access. In the contemporary case, corporations such as Google, Yahoo, and Linden Lab are the owners, and users pay for access to these sites, not only with fees but also by submitting to particular forms of monitoring, thereby trading their valuable personal information and their privacy in exchange for access. Following this, digital enclosures exemplify a shift in conceptualizing privacy as a right to conceptualizing privacy as a commodity to be exchanged for other goods and services (Leman-Langlois 2008; Steeves 2006).

While the term "digital enclosure" is fairly recent, the concept is similar to what media scholar Joseph Turow calls a "walled garden". Both terms are used interchangeably in this chapter. A walled garden is

> an online environment where consumers go for information, communications, and commerce services and that discourages them from leaving for the larger digital world. The concept initially referred in the late 1990s to a safe place for children on the Web; parents would set their computers so that the kids

> could visit only those areas. Quickly, however, the concept morphed to mean an area where content providers could induce targeted consumers to enter—sometimes even have them pay for entry—and then track their activities while surrounding them with ads appropriate to their demographic characteristics and actions (Turow 2005: 117).

Users are enticed to enter and stay in walled gardens through a wide array of premium services that are not easily available on the rest of the internet. America Online (AOL) is a well-known example of a walled garden, complete with desirable content such as music, videos, and online magazines available only to paying subscribers. In return for access to their personal information, AOL blocks spam and unwanted pop-ups, and customizes ads according to the user, the materials they choose, and the time of day (Turow 2005). Subscribers' behaviours are also recorded and analysed in order to tailor content to their inferred tastes.

Second Life is a prime example of a digital enclosure. Countless services are accessible in one site, from financial planning (Wells Fargo Bank has an entire SL island), to university classes (Harvard, Princeton, and MIT all have SL campuses), to music concerts (hosted by Sony BMG) to purchasing a new laptop (Dell Computers has a SL store), to cybersex and escort services. In exchange for convenient access to all these services under one virtual roof, residents and their behaviours are subject to surveillance. Complete records of everything one says and does, their body movements and facial expressions, the people they interact with, the times at which they do so, their consumer preferences, and so on, can be easily collected and analysed.

Linden Lab has relatively strict privacy policies (except in the event that they merge with another company or go bankrupt—then *all* personal user information can be put up for sale), yet data collection in SL is not restricted to Linden Lab and privacy

policies are often ignored. Corporations that have invested millions of dollars to establish their presence in SL use the world to collect significant amount of marketing information (Au 2008a). The ability to harvest the demographic and personal information of users (including their shopping preferences, in-world travel and usage patterns, and even personal conversations) is enhanced by the "open code" of SL that gives users access to the blueprints to the virtual world as well as the ability to modify certain areas. For example, corporations can create "Zombie bots", automated software agents that look like avatars, but are controlled solely by algorithms. These spy bots roam SL collecting data on SL residents (Au 2008b). Providing users, including other corporations, with access to the underlying architecture is intended to promote creativity, but it also has numerous unforeseen effects including enabling enhanced dataveillance of other parties. Residents can have difficulty arguing that these initiatives breach their privacy, as the information is gathered in an ostensibly open forum where there is little expectation of privacy. Further examples of such surveillance include the CIA and other government trolling SL to investigate terrorist activity (O'Harrow Jr. 2008).

While data collection via the Internet is nothing new, what we are seeing is an extension of the depth and breadth of the information being collected. There is a significant difference between collecting data in the physical world, collecting data online in general, and collecting data specifically in digital enclosures such as SL (Zarsky 2004; Zarsky 2006). In the physical world, corporations regularly collect a variety of data about consumers, but this data is generally restricted to a final purchase (e.g. American Express creates profiles based on consumer purchases). Online corporations can track users' actions and browsing patterns using cookies, even monitoring idle surfers who do not

make any purchases. This data is then aggregated and compiled into profiles using sophisticated databasing technologies (Poster 1996). Yet these profiles are not flawless. While navigating the Internet, users divide their attention (and thus the data trail they leave behind them) among several e-commerce vendors, content providers, and other online applications. The profiles that corporations create are limited in scope and prone to errors, as the users they track are constantly logging in and out, creating piecemeal patterns as users move from one website to another. Aggregating data collected at different times, places, and sources into a single profile results in numerous overlaps and errors in the data.

Surveillance in digital enclosures such as Second Life is broader in scope in that it pertains to an extended online experience and monitors a more persistent and detailed online identity. In SL, purchases, education, workplace training, socialization, and dating all occur under the same roof. Because SL residents spend a great deal of time in this monitored environment, much more than they would spend on any one website, the data trail they leave behind—including logs of everyone they ever talked to, every place they visited, and every purchase—is immensely valuable to corporations, especially those who own these virtual worlds.

Total Surveillance Society

In 1974 James Rule proposed a number of criteria to distinguish the surveillance capacity of a society (Rule 1974). In light of technological developments in networking and communication technologies that have emerged since 1974, David Lyon has updated Rule's original categories and depicts the four dimensions of surveillance capacity as 1)

size of data files, 2) comprehensivity of reach in terms of institutional access to data, 3) speed of data flow, and 4) subject-transparency in terms of subject visibility to monitoring (Lyon 1994). Second Life especially, but digital enclosures in general, fit the criteria for a total surveillance society almost perfectly. The fact that these enclosures exist in the realm of data makes the complete collection, databasing, and analysis of residents' data a realizable enterprise, right down to logging every facial expression. While avatars are not used in all digital enclosures, technology analyst firm Gartner, Inc. predicts that by 2011, eighty percent of active Internet users will have avatars. This level of surveillance, especially that enabled by avatars that allow for facial expressions and body language, is impossible in terrestrial space, where many behaviours go unsurveilled and unremarked upon.

Users' anonymity is being slowly pushed aside in favour of transparency. Online anonymity was once taken for granted and valued in terms of encouraging identity exploration and the transcendence of race, gender, and class barriers. Increasingly, however, user's behaviours and lives online are being connected to their offline identities, and users need to censor their behaviours and the information they reveal online. Recent controversial examples include the U.S. military delving into personal emails and online activity logs to "out" gays, and employers performing google searches to provide background on potential employees (Associated Press 2007; Nederlander 2008). A closer look at identification practices and anonymity in SL further highlights the decreasing anonymity in cyberspace.

In the short history of SL, avatars were anonymous. Real world identifiers were not required, and users' off-line identities were protected. All that was needed to create

an avatar account was an email address. In fact, the right to anonymity has always been protected by Linden Lab, as evidenced by their community standards. One of the six cardinal sins is disclosure, "sharing personal information about a fellow Resident—including gender, religion, age, marital status, race, sexual preference, and real-world location" (Linden Lab 2007). Yet, this protection of anonymity is quickly reversing in the face of pressures created by both the growth and corporatization of the space.

More and more, being visible equates to having one's avatar linked to real life identifiers. In order to do business in SL one must increasingly expose one's real world identity as a token of trust (Lyon 2001). Although not initially popular, residents' "First Life" pages are increasingly valued as information sources and indicators of trustworthiness. These profile pages include information on residents' "First Life" (their "real world" identities) such as their names, locations, and occupations. Such information ostensibly determines who is genuinely committed to being part of SL to the extent that they are willing to stake their offline reputation on it. The growing popularity of "First Life" pages coincides with the increasing corporatization of SL (with numerous Fortune 500 Companies such as Cisco, IBM, Dell, Sears, and Reebok attempting to establish their presence in SL). SL contractors who earn a living designing content for these companies must expose their real identities, as businesses and organizations demand that avatars validate their 'true' identities. For example, the avatar Aimee Weber initially preserved the anonymity of her user while brokering SL design contracts with Warner Brothers and American Apparel, but this anonymity was short-lived. Ultimately avatar Aimee Weber "came out" as Alyssa LaRoche in real life in order to secure a SL development contract

with the United Nations. This coming out process is familiar to many SL residents hoping to make a living from their creations (Au 2008a).

The anonymity that SL residents were originally entitled to may also be a thing of the past for all residents, not just those interested in securing employment. According to Robin Harper, Linden Lab VP Community and Support, they are "in the process of implementing an improved electronic age verification system that will verify Residents' ages by using different forms of identification, such as national identification numbers, passports, and social security numbers" (Harper 2007). The implementation of this identification measure coincides with negative media attention surrounding residents who used SL avatars to simulate sex acts such as pedophilia (Harper 2007). Anonymity makes it difficult for Linden Lab to apply sanctions to those who violate the written rules and community norms of SL, and accordingly it is not surprising they are attempting to link avatars to real world identifiers as the virtual world grows in size and gains more media and corporate attention (Whitson and Doyle 2008). While anonymity is seemingly fine for games and role-play, this anonymity is anathema to the latter practices that necessarily involve identity verification, paper trails, and accountability. Accordingly there is a shift from visible, yet anonymous, avatars to avatars that are increasingly linked to their users' offline identifiers and reputations.

Labour and Creative Capitalism in the Digital Enclosure

User-created content, alongside the user information noted above, is a valuable commodity to corporations. While user content creation fosters creativity and productivity, it is the corporations that benefit from and control this labour in digital

enclosures. Users' unpaid labour is a cheap and efficient way for corporations to respond to the demand for increased and improved content, serves to keep existing users from becoming bored, and draws in potential new users. Users' increased creative control results in a stronger identification and emotional investment in the space as well as a hesitancy to abandon it (Humphreys 2007). Corporations portray user labour as a solution to alienation related to mass production and consumption, and persuade users to manufacture content for digital enclosures by promising them that their experience will be more satisfying with increased input, personalization, and effort (Andrejevic 2007: 145). Users, in true neoliberal form, take on the duties of production in order to create a product that addresses their specific desires and needs.

Anthropologist Tom Boellstorff associates user-created content with creationist capitalism, a mode of capitalism in which labour is understood in terms of creativity, and production is accordingly understood as creation (Boellstorff 2008). By framing labour in terms of creativity, work is framed as play (Yee 2006). This trend can be seen in many online sites, including social networking sites such as Facebook and MySpace, as well as YouTube and other digital enclosures that rely entirely on users for content. The valorization of creation is key to Linden Lab's business model as it provides a way around the large development resources required to add new content to SL. For example, in 2006, the total amount of content created by residents was equivalent to the output of 5,100 full-time programmers. This labour is wholly unpaid. Users instead pay Linden Lab monthly fees and property "taxes" for the privilege of creating content (Craig 2006). This leads to uneven property relations that characterize digital enclosures:

> In a traditional Marxist analysis this would be seen as a form of superexploitation where workers are unable to reproduce their needs for

> existence. Within a logic of creationist capitalism, such labor could be seen to have both exchange value and use value as a form of self-fulfillment....Creationist capitalism allow[s] labor to acquire value as a form of leisure (Boellstorff 2008: 213).

The cultural logic of creationist capitalism renders intelligible a "state of affairs where consumers labor for free (or for a nominal prize) to produce advertising materials for a product they have already purchased" (Boellstorff 2008: 210). While there is a cultural significance to content creation and it is a valued skill in SL communities, most creators make little to no money—just enough to pay their taxes, or the equivalent of five or ten dollars a month.

While user-created content can accumulate substantial real world economic value, more things than just economic interest and property rights bind users to digital enclosures. The social networks they establish also ensure that they remain. While there exists a neo-liberal discourse of the empowered consumer who can leave the digital enclosure if not happy with how they are governed or how they as individuals are treated, this ignores the users' role of co-producers of content, their interest in the digital goods and reputations they have accumulated, the community networks they have established and the online identities that they have created. This further exemplifies the uneven relations that are created by digital enclosures.

Linden Lab, seemingly on the side of users in terms of instilling intellectual property rights and claiming that SL is "imagined, created, and owned by its residents", is one of the worst offenders. Linden Lab promotes the image of a self-governing community where residents can profit from their creativity, yet most of the profit goes directly to Linden Lab. By signing SL's Terms of Service (TOS) before they enter, residents agree that Linden Lab can pull the plug of the world, their avatars, and their

considerable investments in the world without any legal liability or means of recourse. In fact, Linden Lab quietly dropped the "owned" from its tagline in 2007, thereby de-emphasizing the rights of ownership, if any, that residents may have in SL. The complex property relationships between corporations and users point to the need to rethink previous theorizations of the relationship between property, ownership, and power online. Although it is beyond the scope of this paper to develop this extensively, we require a new political economy of online spaces that takes into context the new network of property relations enabled by user-created content. Parallel to the real world, and despite the important role played by users-as-content developers, the powerful still impose their will on property relations.

Creative capitalism extends the surveillant capacities of digital enclosures by encouraging residents to develop and post their own content. This content deepens and broadens corporate dataveillance even further by incorporating residents' writing, chat logs, and digital designs into the surveillant gaze. A hidden aspect of user-created content is how it facilitates a participatory form of surveillance (Albrechtslund and Dubbeld 2005; Leman-Langlois 2008; Taylor 2006b). A sizeable proportion of users engage in behaviours with the purpose of letting third parties watch their activities, for exhibitionist pleasure, personal pride, and communication. Although data from the digital enclosure may not always point directly to a specific physical individual, it does track a generally persistent identity—such as one's avatar—over extended periods of time. This level of surveillance has significant implications for the freedoms traditionally associated with the Internet and with convivial technologies.

Total(itarian) Surveillance Society

Digital enclosures are not just total surveillance societies but *totalitarian* surveillance societies as well, where corporations exert total control over each enclosed online space. This section further highlights the uneven power hierarchy that exists between users and corporations. While John Perry Barlow applauded the fact that the Internet has no elected government, the absence of this government creates opportunities for exploitation. Democracy, in part, is reliant on a symmetry of relations. In exchange for citizen's votes, elected governments are mandated with carrying out the will of the public and remain accountable to the public. There is a symmetry of visibility wherein rulers provide the public with access to their deliberations and the policy they form. Corporate rulership, is by contrast, asymetrical: the decisions and actions of corporate entities remain opaque even as users are rendered increasingly transparent to marketers and advertisers. Rather than accountability and transparency, corporate digital enclosures offer the promise of convenience and customization as an alibi for a shift in power relations: "for the ability to discriminate invisibly and to gather information that facilitates market management and public manipulation" (Andrejevic 2007: 258).

Much of the asymmetry between corporations and users is a result of an imbalance in visibility. While the corporate ruler "sees all and knows all," including the minutia of residents' day to day lives online, their own practices and policies are opaque. This has important implications for online privacy given that legal privacy rights are primarily focused on the state. Corporations such as Linden Lab are just one example of a non-state agency conducting surveillance limited, for the most part, only by the "fair information practices" they have chosen to instil, which in themselves have only a limited

record of success (Ericson and Haggerty 2006). David Brin argues that a synoptic form of surveillance may reverse some of the power imbalances between the watched and the watchers, in this case, corporations and users (Brin 1998), but as of yet, there are few ways for users to turn the surveillant gaze upon the corporate deities that operate digital enclosures. It is difficult to be optimistic about the idea of a transparent society (a society that allows everyone equal access to information) given that large corporations continue to operate behind closed doors and few privacy laws actually have an impact upon their practices.

While corporations are happy to collect users' information under the guise of improving service, users encounter difficulties when challenging the way digital enclosures are governed. Linden Lab replaced the open forums of SL with blogs that allow only corporate employees to post (Boellstorff 2008), and there are few opportunities for residents to discuss their concerns with Linden Lab staff given the decreasing staff presence in SL (Au 2008a). The significant history of protests and demonstrations in virtual worlds points to an alternate method of representation. Masses of protesting avatars have presented a united front that catches the attention of the corporations, as well as the media. Collective action is relatively common, and there are many accounts of users rallying to pressure companies to address problematic issues. For example, an early protest in SL recreated the Boston Tea Party as a means to protest Linden Lab's taxation policy. Shortly afterwards the policy was rescinded (Au 2008a). When Linden Lab did not respond quickly enough to a "copybot" program that duplicated residents' designs and violated intellectual property rights, shopowners closed their shops in protest (Gonsalves 2006). IBM's move to Second Life was quickly

followed by an in-world protest in September 2007 by workers at IBM Italy that led to international press coverage and the resignation of IBM Italy's CEO. Following that success, union members again rallied for collective action, this time in response to IBM outsourcing labour contracts. The repercussions of this protest were not restricted to the virtual world—the strike was noted by AOL's stock market resource webpage, which consequently sent waves of shareholders and potential investors searching the internet for more information (Au 2008c).

Although at first glance such examples provide encouraging signs of democratic potential, not all public demonstrations are successful. In fact, they are more often met with severe repercussions, as officials frame protests as a disruption of the digital enclosure, a violation of the terms of service, and an offence that ultimately leads to protesters' accounts being closed and their avatars destroyed (Taylor 2006a). T.L. Taylor, for example, details the corporate response to a protest in an online game, World of WarCraft:

> It was not met with a positive reception by Blizzard, the developers and maintainers of the game. Not unlike the kinds of warnings you expect to hear offline from police at unsanctioned demonstrations, participants at the protest were told by a Blizzard representative via the in–game communication system:
> *Attention: Gathering on a realm with intent to hinder gameplay is considered griefing and will not be tolerated. If you are here for the Warrior protest, please log off and return to playing on your usual realm. We appreciate your opinion, but protesting in game is not a valid way to give us feedback. Please post your feedback on the forums instead. If you do not comply, we will begin taking action against accounts. Please leave this area if you are here to disrupt game play as we are suspending all accounts* (Taylor 2006a, emphasis added).

Companies argue that such gatherings stress the technical limitations of the digital enclosure, result in slowed server response and the potential for server crashes, and

consequently endanger other users' enjoyment of the space. Because of this, the companies argue, collective action must be halted in order to prevent server crashes and to avoid inconveniencing users who are not participating in the protest. In addition, collective action is seen to violate the end user licensing agreements (EULAs, otherwise known as the Terms of Service) that users must accept prior to entering the virtual world. Accordingly, there are few options for users to provide input into how they are governed in digital enclosures.

Game designer Richard Bartle has written extensively on the uneven power hierarchy that exists between corporations and users. This hierarchy is rooted in the relative ease with which coded rules can be used and altered by corporations to govern populations. The scope of corporations' powers is reflected in the following quote:

> Virtual worlds are played by rules. The rules are written (embodied in the code) and unwritten (embodied in the expectations of the players). People can deny the existence of unwritten rules, but they can't deny the existence of coded rules....You may be able to pick and choose which cultural norms to obey, but you don't get to pick and choose which rules of the virtual world's physical universe to obey—and the administrator's authority in a virtual world is embodied in those rules. You don't swear, because if you do you're disintegrated. You don't do anything that the administrator doesn't want you to do, because if you do you're disintegrated (Bartle 2006a: 36-37).

Most legal scholars equate corporate administrators to the governments of online spaces (Balkin 2006; Castronova 2006; Lastowka and Hunter 2003). It matters little whether these governments are elected or not. What matters is their unrestricted power to govern online populations.

Corporations are granted ownership of online identities, labour, and user information through the terms of service and EULAs that users must accept before entering. These companies are not accountable or transparent, and their rules are often

opaque even to terrestrial courts and legislation. Accordingly, they make *de facto* law (Humphreys 2007). Their powers are so absolute that it is argued that they are not governments at all, who could be disposed of by the populace, but rather dictators (Boellstorff 2008: 222; Doctorow 2007) and gods (Bartle 2006b). The monopoly on force and coercion, traditionally held by the state alone, has been handed over to private parties. Corporations can "banish" users without recourse, drastically alter the physics and mechanics of the digital enclosure, or destroy it at will. Given that these digital enclosures account for an increasing proportion of online spaces, and that our lives are increasingly lived online, this is a worrying trend.

Conclusion

While John Perry Barlow applauds the fact that the Internet has no elected government, this means that the tenets of democracy that constrain most governments in the terrestrial world do not apply. The symmetry of relations, accountability, and transparency associated with terrestrial governments, and with democracy in general, are absent. There is no public scrutiny of corporate-cum-government decision making, policy, and actions. Corporations have low levels of accountability to on-line communities and ban users at will, denying them access to their communities, their user created content, and their online identities without any requirement that their decision-making process be transparent or open to contestation by users who feel that they have been wrongly punished. The current proprietary environment that gives corporations the power to banish users without any transparent governance process and the power to alter code and erase entire online domains at the flip of a switch ultimately ends up with users governed

through the threat of losing their online identities, communities, and virtual property. While consumer activism is sometimes effective, there is little recourse if protests fail. In the terrestrial world, exploited and unhappy citizens have the rule of law, they can sue and they can elect new leaders. Users of digital enclosures lack these rights.

The forms of participation and empowerment open to users are harnessed to corporate drives for efficiency and profitability. Rather than working to correct power asymmetries in society, as predicted by the decentralized model of the Internet, the Internet contributes to ever-increasing levels of surveillance, concentrates power in the hands of a few, and erodes transparency and openness. While the Internet is seen as democracy-promoting in terms of how it affords potentials for political organization from below, it is increasingly important to examine how new media is appropriated for corporate ends, and how this alters the democratic potential of the Internet. Moreover, it is increasingly important to examine how citizenship is constantly being redefined in online spaces. Consumer relationships are replacing other practices of community and government, and act as a stand-in for true citizenship. Digital enclosures are one way in which the labour and information of online "citizens" are being exploited under the guise of community and creativity.

Works Cited

Albrechtslund, Anders and Lynsey Dubbeld. 2005. "The Plays and Arts of Surveillance: Studying Surveillance as Entertainment." *Surveillance & Society* 3:216 - 221.

Andrejevic, Mark. 2007. *iSpy: surveillance and power in the interactive era*. Lawrence: University Press of Kansas.

Associated Press. 2007. "U.S. Military Continues to Discharge Gay Arab Linguists, and Congress Members Seek Hearing." in *International Herald Tribune*.

Au, Wagner James. 2008a. *The making of Second Life: notes from the new world*. New York: Collins.

—. 2008b, "Metaverse Bots: How To Spot Them, What To Do With Them?" Retrieved April 1, 2008 (http://nwn.blogs.com/nwn/2008/02/bots-how-to-spo.html#more).

—. 2008c, "Virtual World Labor Protest Shows Up On IBM's Real World Stock Chart", Retrieved March 31, 2008 (http://nwn.blogs.com/nwn/2008/03/virtual-world-l.html).

Balkin, J. M. 2006. "Law and Liberty in Virtual Worlds." Pp. 86 - 117 in *The state of play: law, games, and virtual worlds*, *Ex machina*, edited by J. M. Balkin and B. S. Noveck. New York: New York University Press.

Barlow, John Perry. 1996, "A Declaration of the Independence of Cyberspace", Retrieved August 22, 2008 (http://homes.eff.org/~barlow/Declaration-Final.html).

Bartle, Richard A. 2006a. "Virtual Worldliness." Pp. 31 - 54 in *The state of play: law, games, and virtual worlds*, *Ex machina*, edited by J. M. Balkin and B. S. Noveck. New York: New York University Press.

—. 2006b. "Why Governments aren't Gods and Gods aren't Governments." *First monday*.

Boellstorff, Tom. 2008. *Coming of age in second life: an anthropologist explores the virtually human*. Princeton: Princeton University Press.

Brin, David. 1998. *The transparent society: will technology force us to choose between privacy and freedom?* Reading, Mass.: Addison-Wesley.

Castronova, Edward. 2006. "The Right to Play." Pp. 68 - 85 in *The state of play: law, games, and virtual worlds*, *Ex machina*, edited by J. M. Balkin and B. S. Noveck. New York: New York University Press.

Craig, Kathleen. 2006. "Second Life's Must-Have Stuff." in *Wired*.

Doctorow, Cory. 2007. "Why Online Games are Dictatorships." in *Information Week*.

Ericson, Richard V. and Kevin D. Haggerty. 2006. *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

Galloway, Alexander R. 2004. *Protocol: how control exists after decentralization*. Cambridge, Mass.: MIT Press.

Gandy, Oscar. 1993. *The panoptic sort: a political economy of personal information*. Boulder, Colo.: Westview.

Gonsalves, Antone 2006. "Second Life Shop Owners Threaten Suit Against Virtual World's Creator." *Information Week*, November 15.

Harper, Robin. 2007, "Accusations Regarding Child Pornography in Second Life", Retrieved November 1, 2007

Humphreys, Sal. 2007. ""You're In Our World Now." TM: Ownership and Access in the Proprietary Community of an MMOG." Pp. 76 - 96 in *Information*

Communication Technologies and Emerging Business Strategies, edited by S. Van Der Graaf and Y. Washida. London: Idea Group Publishing.
Lastowka, F. Gregory and Dan Hunter. 2003. "The Laws of the Virtual Worlds." University of Pennsylvania Law School.
Leman-Langlois, Stéphane. 2008. "Privacy as Currency: Crime, Information and Control in Cyberspace." in *Technocrime*, edited by S. Leman-Langlois: Willan.
Linden Lab. 2006, "Second Life Homepage", Retrieved December 29, 2006 (www.secondlife.com).
—. 2007, "Community Standards", Retrieved April 21, 2007 (http://secondlife.com/app/help/rules/cs.php).
Lyon, David. 1994. *The electronic eye: the rise of surveillance society*. Minneapolis: University of Minnesota Press.
—. 2001. "Under My Skin: From Identification Papers to Body Surveillance." Pp. 291 - 310 in *Documenting individual identity: the development of state practices in the modern world*, edited by J. Caplan and J. C. Torpey. Princeton, N.J.: Princeton University Press.
Monahan, Torin. 2008. "Surveillance, Social Control, and Democratic Governance." in *Surveillance and Democracy*, edited by M. Samatas and K. Haggerty. Rethymnon, Crete.
Nederlander, Ned. 2008, "One in Five Employers Scan Applicants' Web Lives", Retrieved Sept 13, 2008 (http://tech.slashdot.org/article.pl?sid=08/09/11/208206).
O'Harrow Jr., Robert. 2008. "Spies' Battleground Turns Virtual: Intelligence Officials See 3-D Online Worlds as Havens for Criminals." Pp. D01 in *Washington Post*, vol. February 6. Washington.
Poster, Mark. 1996. "Databases as Discourse; or, Electronic Interpellations." Pp. 175 - 192 in *Computers, surveillance, and privacy*, edited by D. Lyon and E. Zureik. Minneapolis: University of Minnesota Press.
—. 2004. "The Information Empire." Pp. 317 - 334 in *Comparative Literature Studies*, vol. 41: Pennsylvania State University Press.
Rheingold, Howard. 2000. *The virtual community: homesteading on the electronic frontier*. Cambridge, Mass.: MIT Press.
Rule, James B. 1974. *Private lives and public surveillance; social control in the computer age*. New York: Schocken Books.
Steeves, Valerie. 2006. "It's Not Child's Play: The Online Invasion of Children's Privacy." *University of Ottawa Law and Technology Journal* 3:169 - 188.
Taylor, T. L. 2006a. "Beyond Management: Considering Participatory Design and Governance in Player Culture." *First monday*.
—. 2006b. "Does WoW Change Everything? How a PvP Server, Multinational Player Base, and Surveillance Mod Scene Caused Me Pause." *Games and Culture* 1:318 - 337.
Turow, Joseph. 2005. "Audience Construction and Culture Production: Marketing Surveillance in the Digital Age." *The Annals of the American Academy of Political and Social Science* 597:103 - 121.
Whitson, Jennifer and Aaron Doyle. 2008. "Second Life and Governing Deviance in Virtual Worlds." in *Technocrime: Technology, Crime, and Social Control*, edited by S. Leman-Langlois. Cullompton, Devon: Willan Publishing.

Yee, Nick. 2006. "The Labor of Fun: How Video Games Blur the Boundaries of Work and Play." *Games and Culture* 1:68 - 71.

Zarsky, Tal Z. 2004. "Information Privacy in Virtual Worlds: Identifying Unique Concerns Beyond the Online and Offline Worlds." *New York Law School Law Review* 49:231 - 270.

—. 2006. "Privacy and Data Collection in Virtual Worlds." Pp. 217 - 223 in *The state of play: law, games, and virtual worlds*, *Ex machina*, edited by J. M. Balkin and B. S. Noveck. New York: New York University Press.