Article

Second Life Surveillance: Power to the People or Virtual Surveillance Society?

Jennifer Martin

University of Western Ontario, Canada. jmart9@uwo.ca

Abstract

In the virtual world of Second Life, almost all content is user-generated and users retain a significant amount of autonomy. Given this freedom, participants are able to create, acquire, and use their own forms of surveillance. With accessible, affordable, and easy to use options, ordinary participants regularly deploy surveillance to protect themselves and their interests, businesses, and property. This paper examines the applications, awareness, and climate of surveillance within the virtual world. It argues that the socio-technical environment of Second Life facilitates problematic covert surveillance, but also makes possible forms of resistance. Examples of surveillance technologies and applications reveal the ways in which the virtual world supports and obscures surveillance, making these practices challenging for participants to detect, analyze, and respond to. However, the recent controversial case of RedZone not only highlights some of the most pressing issues with Second Life surveillance, but also the ways in which participants are able to respond to perceived threats. Although ostensibly intended to track Internet protocol (IP) addresses in order to prevent in-world harassment and theft, participants expressed widespread concern at the program's potential for associating online and offline information and for linking together different avatars. In doing so, awareness was raised, protests were made, and counter-technologies were developed. These responses point to the ways in which the virtual world makes possible resistance to surveillance practices, especially when they are seen as a threat or intrusion.

Surveillance in Second Life

In the virtual world of *Second Life* (SL), a device the size of a pixel can be attached to a participant's avatar so unobtrusively that it is unlikely that the user will notice. In spite of its small size, this device is capable of conducting detailed and complex surveillance. Beyond noting the identity of the individual to whom it is attached, this device can also track their movements within the world and relay any conversations they and the people around them have back to the individual who attached it. The resident, however, may never know that it is there, at least until the consequences of their surveillance become personally or professionally apparent.

To date, there is little work on either the potential for or repercussions of surveillance in virtual worlds like *Second Life*. However, with millions of users taking part in virtual worlds (Reahard 2011; Linden Lab 2011) and billions of dollars in revenue from virtual goods (Smith 2011; Linden Lab 2011), virtual surveillance and privacy are major concerns for many *Second Life* participants, who are usually referred to as "residents." Because the virtual world is different from offline life in many ways, and affords different interactions between users, it is necessary to consider surveillance within this new context, and to consider how the virtual world makes surveillance possible as well as the ways in which participants are aware of and responding to these practices.

Surveillance can take a number of different forms and serve a variety of purposes. The recent controversial case of RedZone, a surveillance program that detects and records Internet Protocol (IP) addresses, highlights some of the most pressing issues with surveillance in *Second Life*, but also points to the ways that such technologies are discussed and resisted by participants who are aware of and concerned about their implications. In contrast, other examples reveal the ways in which specific social and technical features of the virtual world helps to support and obscure “in-world” (i.e. in *Second Life*) surveillance, making these practices difficult for SL participants to detect, analyze, and respond to. When considered together, these examples serve to demonstrate not only how the socio-technical environment of *Second Life* facilitates problematic covert surveillance, but also the ways in which resistance is made possible.

The Threats of Virtual World Surveillance

Second Life is a virtual world that is based almost entirely on user-generated content. Participants are given a large degree of freedom not only to use the world in almost any way they see fit, but also to create within it. In many cases, user-generated content is focused on creating virtual items such as clothing, hair, houses, cars, and pets. These goods can all be used, given away, and even sold to other participants within the world. However, this freedom also allows for participants to develop their own programs and scripted devices. It is here that surveillance technologies come into play, with users creating or buying and using their own surveillance devices capable of anything from announcing when another participant has arrived in a particular area to remotely recording conversations. With its reliance on user-generated content, *Second Life* allows for a form of lateral surveillance, “understood as the use of surveillance tools by individuals, rather than by agents of institutions public or private, to keep track of one another” (Andrejevic 2005, 488).

Since it is a virtual world, the threats and risks associated with surveillance in *Second Life* are somewhat different than those experienced in offline life. In offline life, surveillance is becoming nearly ubiquitous. Individuals are surveilled in terms of where they go (Prosen 2006), what they do (Slobogin 2002), who they call (Stillwagon 2007-2008), where they go online (Barnes 2005), and almost anything else that can be monitored. Within a surveillance society, it is difficult if not impossible to escape surveillance (Lyon 2001). Surveillance is often seen in a bureaucratic context (Gandy 2006), and as a way to monitor individuals in order to moderate or reduce risk or threat (Lyon 2001). It also functions in a Foucauldian, panoptic sense as a form of social control, by encouraging individuals to anticipate surveillance and corrective intervention, and therefore behave in predictable and approved ways (Campbell and Carlson 2002).

Second Life surveillance functions as a limited form of social control in that it is intended to manage participants in particular ways, such as tracking them and blocking them from designated areas of the world or monitoring where participants go and what they say. However, much of the surveillance in *Second Life* is not apparent as a tool of bureaucracy or of a more universal social control. Because participants conduct surveillance in a world that, apart from the rules imposed by its developers, is lacking in government or governance, it does not have the bureaucratic characteristics of offline surveillance. At the same time, it is not usually consistent enough, nor visible enough, to ensure the widespread awareness and consequent social control usually seen within the surveillance society. Instead, surveillance is targeted to more individual and personal needs: keeping problematic participants away from land, tracking suspected philanderers, monitoring in-world partners, recording personal conversations, and logging visitors to particular destinations.

The most significant difference between offline and online surveillance, and the one that makes considering surveillance in virtual worlds so important, is the role of privacy. Surveillance is often considered in terms of its threat to privacy in everyday life (Flaherty 1992; Slobogin 2007). These

discussions focus on the gradual disappearance of privacy, and the fact that the elements of life that are not in some way surveilled are diminishing (Lyon 2001). In this sense, this work also acknowledges that there are fewer outlets available to individuals for escape. Within this context, *Second Life* offers a space that reestablishes a level of privacy. Furthermore, it facilitates freedom and exploration for participants in a way that is highly valued.

Both the perception and expectation of privacy are high in *Second Life*. Because the world allows for anonymity, no one ever need know who is the individual behind the avatar. Unless the individual offers this information, the only thing that definitively links an avatar to the offline individual is their IP address and credit card. If they use a free account—which around 90 percent of residents do (Llewelyn 2008)—or a credit card other than their own, their IP address is the only link between both identities. Similarly, the IP address is also the only thing that associates multiple avatars used by the same individual with each other. Therefore, although there are some concerns around the threat to virtual businesses created by surveillance (Au 2007) what many participants perceive to be the biggest threats based on the frequency, length, and content of their forum and blog discussions are often more personal, such as tracking personal information like IP addresses, making connections between their multiple avatars, or linking the avatar to the offline individual as a form of “outing.”

For many participants virtual worlds become important spaces for engaging in identity exploration and play, which offers opportunities not only to try out and explore different versions of the self (Turkle 1995; Kafai, Fields, and Cook 2010), but also to reveal the “true self” that some individuals may have a difficult time expressing in their everyday lives (Bargh, McKenna, and Fitzsimons 2002; McKenna, Green and Gleason 2002). Many people experience a sense of identification with and attachment to their virtual self (Turkle 1995; Blinka 2008), even to the point where negative things that happen to the avatar are experienced as harm (Wolfendale 2007). Virtual worlds also become places where participants are able to explore activities and preferences that are more difficult or challenging in their offline lives (Bugeja 2007; Brookey and Cannon 2009; Bardzell and Barzell 2006). *Second Life* therefore makes possible options that are difficult or challenging if not impossible in participants’ offline lives.

Surveillance in *Second Life* threatens to disrupt the privacy that makes these explorations, interactions, and experiences possible. Privacy is the ability of an individual to control their personal information and to determine what information is available about them and how it is used (Shapiro and Baker 2001). Given that *Second Life* enables and even encourages the creation of alternate selves, privacy is associated with protecting both in-world and offline personal information. While control is relevant in terms of protecting information in its own right, it also extends to ensuring that personal information is not used to associate different and varied identities together if participants do not wish for these links to be known. Any such exposures potentially undermine the privacy of the virtual world and participants’ abilities to engage in it in the ways that they desire and that are useful to them.

Given the various roles that the virtual world serves for participants, privacy becomes a very important element of virtual life. In-world surveillance can have online and offline repercussions for those who are subject to it. Because in-world anonymity is possible and participants can simply not engage in the world, walk away, or create another avatar, privacy and surveillance may not immediately be seen as pressing concerns or, at least, concerns that are as significant as those raised in relation to offline surveillance. However, these potential violations of participant information do have implications for both in-world and offline privacy and security that are worth considering, especially in light of their repercussions within a space that is heavily valued by participants.

To consider these effects, the author conducted content analysis of the official *Second Life* forums (<http://community.secondlife.com/>), *SLUniverse* forums, (www.sluniverse.com/) and established and relevant blogs such as *New World Notes* (nwn.blogs.com/), *Virtual Navigator*

(<http://virtualnavigator.wordpress.com/>), and *no2redzone* (<http://no2redzone.wordpress.com/>). This analysis was initially conducted during the rise in awareness of and critical response to RedZone from February to March of 2011, and then revisited in December of the same year. With over 11700 responses to forum threads dealing with certain elements of in-world surveillance in addition to numerous blog posts and blogs, participants actively consider and discuss these practices.

By considering both the quantity of discussion and the ways in which surveillance is addressed in relation to different technologies and applications, this approach reveals participant awareness of and concerns around the use of surveillance within the virtual world. Within these venues, participants provide opinions, thoughts, and observations in their own words. As a result, these sites served as sources of information on what individuals are thinking about in terms of in-world surveillance. Because this commentary is voluntary, it offers a useful way to consider participant's perceptions of surveillance. In addition, the frequency with which they are introduced and the extent to which they are discussed also reveals the relative importance of different topics.

The Case of RedZone

RedZone is a program that offers a useful case study for considering surveillance in *Second Life*. Released in the summer of 2010, RedZone was an application intended for use in the virtual world. It sold on the *Second Life* marketplace for \$3999 Linden dollars—the world's virtual currency—a price that is equivalent to about \$17 USD. Because it was sold on the marketplace, the application was available to any participant who was willing to pay. Initially, the program proved popular, especially given its claims to assist content creators and landowners who wished to protect their in-world assets by banning troublesome participants and those who threatened to copy their work. Although exact sales figures are unavailable, estimates suggest that over 20 000 copies of the program were sold (Rhiadra 2011). RedZone was ostensibly intended to identify and block problem residents from visiting particular “sims”—the term used to describe *Second Life*'s land—even when using their alternative avatars—usually referred to as “alts.” Problem residents were defined as general troublemakers—usually referred to as “griefers”—and those who were using CopyBot, a program that copies and replicates virtual goods in violation of the world's Terms of Service (ToS). When an avatar visited a sim running RedZone, the program would use the built-in streaming media service to locate their IP address. When avatars engaging in griefing or copying were detected, the IP address of the alleged culprit was entered into the program's database. If another avatar using the same IP address attempted to enter an area using RedZone, their IP would be checked against those in the database. If a match was found, that avatar would be banned not only from the sim they were attempting to enter, but also from any sim running RedZone.

As one of the most recent and extensively discussed in-world surveillance technologies, RedZone not only reveals the issues surrounding in-world surveillance and participant concerns, but also illustrates how the socio-technical environment creates spaces for both surveillance and resistance to surveillance. Lyon defines surveillance as “any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered” (2001, 2). The fact that RedZone compared IP addresses and banned all avatars with the same IP address indicates a way of managing individuals who were perceived to be a threat. At the same time, the program also potentially promoted a form of “anticipatory conformity” (Norris and Armstrong 1999), dissuading other participants from causing trouble.

While this program effectively prevented one problem resident from repeatedly returning to the same sims as different avatars, at least as long as she used the same Internet connection, its “collateral blockage” is possibly much wider. Initially, some participants were irritated at the potential for false positives. Dynamic IP addresses, logging in from a shared Internet connection, or using proxy servers or publicly available Internet access could link together avatars that were not actually linked to the same individual.

This meant that some residents were banned from sims because of the actions of other participants who had at some point shared their IP address. As one participant notes, “I ended up on RedZone's ban list without ever touching a copybot” (Kuramoto 2011). In these cases, the inaccuracy of the system was seen to be an issue in terms of banning innocent residents from sims, but also associating them with inappropriate activities in ways that some perceived to be an “insult” (Lili 2011).

The other issues, though, and those that were more extensively discussed in *Second Life* forums and blogs, was the tracking of IP addresses and with it, the linking together of avatars based on this information. Some residents were concerned about the tracking of IP addresses, and whether this could be considered identifying information. Given that tracking IP addresses can be used to determine approximate locations, some participants were concerned about being located and even harassed in their offline lives. As one participant explains, “In the real world my only concern is that you could see where I live. That would be a real problem, since I have a static IP that when you look it up, shows my location within 50 meters of my home. There is only one house even close to mine” (Lili 2011). While many participants indicated that dynamic IP addresses and the general difficulty with tracking someone based on IP alone assuaged most of their fears, some are aware that their particular circumstances mean that this kind of IP-based tracking and identification would be possible.

However, the more prevalent issue discussed by participants was the linking together of avatars, which was in turn linked to issues with both online and offline life. Within forum and blog discussions, participants who take issue with RedZone most commonly argue that their most significant concern is not the tracking of IP addresses in and of itself—a practice that is recognized as a common element of any online activity—but rather the association of different avatars based on a shared IP address (“Redzone: The WitchHunt.what's the REAL issue here?” 2011). For instance, in responding to a forum thread asking whether RedZone really was a significant issue, out of the first 100 responses four specifically mentioned the tracking of IP addresses and their links to offline information and location and three mentioned the violation of the world's ToS. In contrast, 30 responses expressed or agreed with assertions that the most significant issue was the fact that alts could be associated with each other. Although admittedly skeptical about some of these issues, Wagner James Au also acknowledged a number of comments on a RedZone post raising similar points, stating that, “As many readers point out in Comments, as significant a privacy concern as IP tracking (if not moreso) is the way RedZone is able to connect Second Life users with their alt accounts” (2011).

Because RedZone was based on IP addresses, avatars using the same address would be linked together in the program's database. This association became a significant concern for participants who wished to keep their avatars separate and unassociated with each other. As one participant suggests, the issue is not so much the tracking of IP address itself, rather “the point is that this device lets people discover other users' alternate accounts” (Obscure 2011). Another asserts that, “it doesn't matter if I wanted to partner 10 people on 10 different alts, all cheating with a different furry vampire goat, it's NO ONE'S business but my own” (Magic 2011). By linking together avatars, residents feel that their privacy in the virtual world is threatened, especially in regards to the freedom to have different alts, try different things, and, as one participant suggests, “Explore and have Adventures” (“Redzone: The WitchHunt.what's the REAL issue here?” 2011).

The second issue is one that builds on the first. For some residents, an avatar is strongly associated with their offline, or “real life” (RL), identity. Knowing the offline identity of one avatar means that any additional avatars can be associated with that individual. These associations can reveal group memberships, affiliations, activities, and other preferences that the individual may not want to have known for any number of reasons. One participant tries to clarify this point by providing an example:

Imagine I'm employed by ACME University, which has a presence in SL. I am on their PR team, both in SL and in RL and I often telecommute...RedZone will couple my private avatar to my corporate avatar through my home IP address. This is a breach of RL privacy, as my employer has my RL information and can access RedZone to discover the identity of my private avatar" (McMasters 2011).

Later in this thread, the same participant offers a series of questions that again raise similar points about the potential links that can be made between residents and offline life based on RedZone:

If I walk into your SL store, what information about me do you have the right to know? Do you have a right to know I'm a disabled, which you might discover if I have an alt that heads up an SL support group for the wheelchair bound? Do you have the right to know who my employer is, which you might discover if I have an alt that acts as a representative of my employer in SL? If I approach you in-world as a business representative for my company, do you have a right to know the name of my RL husband, who's partnered to my private alt?" (McMasters 2011).

Although some participants' concerns are focused on the in-world implications of linking together avatars, others also account for the potential consequences if avatars are linked to offline identities, especially if they are engaged in particular groups or activities.

RedZone is a surveillance technology of which many *Second Life* residents were (and are) aware and wary. The many discussion threads and blog posts about RedZone make evident that this technology is a concern. This concern arises partly because the program tracks IP addresses, but also because of what is done with those addresses and how they are used. Due to the links that are made between avatars, this program is seen as a threat to the freedom and privacy that is not only enjoyed by participants, but that also serves a very important factor in engaging, interacting, and exploring within the virtual world.

Other In-world Surveillance

Although concerns around false positives and the ability to locate individuals using their IP address were raised, it was largely the potential to link together avatars that caused concern for *Second Life* residents. The example of RedZone is especially telling when compared with other examples of in-world surveillance that, while they do pose other threats, do not track IP addresses or threaten to link together avatars. Although RedZone was extensively discussed through *Second Life* forums and blogs, other surveillance technologies have not been subjected to as much scrutiny despite their presence and use within the world.

Additional forms of surveillance in *Second Life* are important to consider for two main reasons. First, there are in-world surveillance technologies that function in different ways and therefore raise problems not seen with a program like RedZone. Second, when compared with the level of awareness and response to RedZone, other technologies help to further demonstrate the ways in which the socio-technical environment serves to obscure and downplay the use of in-world surveillance.

In addition to RedZone, *Second Life* hosts a variety of other surveillance technologies. Some technology is used for business purposes, such as corporate espionage against companies who conduct business in the virtual world (Au 2007). In general, "The availability of a market in virtual goods trading provides criminals with financial incentives to offend" (Makkai 2009), and surveillance helps to gather sensitive information. By using surveillance around in-world activities such as planning sessions or meetings with vendors or clients, information can be gathered on businesses that operate solely within the virtual world, or on offline corporations that use the virtual space (Taylor 2009). Surveillance is a threat to the integrity

of businesses, both in terms of their information and with respect to private information about vendors, clients, or projects (Au 2007). Those conducting surveillance in *Second Life* could steal enough information to seriously damage the virtual or offline business life of a resident.

These technologies are also used for more personal ends. ChatSpy, for instance, is a program that can be embedded in virtual goods, such as a shirt or necklace, and that tracks the location and records the conversations of the avatar to whom it is attached. Some devices can be attached directly to an avatar, and are so small that they are difficult to detect. Other programs allow residents to record who has visited a particular sim, to track partners who are suspected of cheating, or to listen in on conversations.

These programs allow for the surreptitious collection of resident information. Although they do not usually rely on IP addresses, they are capable of gathering enough information about residents to perform a similar function to RedZone by linking together different avatars or by linking avatars to offline individuals. The threat of these technologies is further increased when individuals who are unaware of their presence divulge personal information. Such devices can easily record information such as offline name, alt accounts, or personal email address that may be shared in confidence with other residents. Given that research on virtual worlds and online interaction indicates that participants regularly give identifying information to others, unrecognized surveillance can be an issue. For instance, 85 percent of people in a Habbo Hotel study knew the real names of most of their in-world friends (Slot 2009). Similarly, researchers note that, “users often divulge personal information, location, education level and occupation to other players when there is some establishment of trust between users” (Dudley et al. 2010). As a result, it is not unusual for virtual world participants to offer identifying information that could be intercepted by surveillance technologies.

Discussions of Surveillance

Although it is only one of many technologies that are used for surveillance in *Second Life*, the awareness and discussion seen around RedZone is markedly greater than seen with other surveillance practices. Because of the perceived threat of the technology, its widespread use, and its use of IP addresses and a database of information, it has been heavily debated amongst *Second Life* residents in terms of their most pressing concerns and how it can most effectively be avoided or dealt with.

RedZone is the most discussed surveillance technology in *Second Life*. As of December 2011, on the official *Second Life* forums there were over 1240 responses in 80 threads that mention RedZone, with over 25 threads dedicated specifically to discussing the technology and its repercussions and tracking efforts to remove it from the world. High levels of discussion are seen in the over 10 500 responses to threads dealing with RedZone on the *SLUniverse* forum. In contrast, ChatSpy programs that track avatar locations and record conversations receive only 63 specific mentions in the current official forums and 50 in the archive, along with an additional 34 at the *SLUniverse* forums.

Discussions of more general surveillance issues appear, at first glance, to be more prevalent than those associated with specific technologies. For instance, surveillance has 93 mentions in the current official forums and 243 in the archive. On *SLUniverse*, there are 1270 posts that refer to surveillance. However, the focus of these posts is very rarely on surveillance in *Second Life*. Rather, these threads deal with general issues, such as Facebook and Google+ privacy, surveillance in everyday life, news coverage of surveillance, and advertisements for new surveillance programs that are for sale.

RedZone posts are also more frequently viewed and responded to than those dealing with other surveillance technologies and programs or with more general surveillance topics. For instance, an official *Second Life* forum thread on banning RedZone from residential areas has 56 replies and 1621 views. Another dealing with the banning of the technology has 81 responses and 3084 views, while a single

SLUniverse thread questioning the disclosure of alts through RedZone has 10 520 responses. In contrast, two of the more popular ChatSpy threads on the official forums have 25 and 5 responses and 110 and 251 views, respectively, while the only dedicated ChatSpy thread on *SLUniverse* has 124 responses. In both the official forum and *SLUniverse*, the quantity of discussion of RedZone is high, while coverage of other surveillance technologies is relatively low.

This discrepancy in discussion is also prevalent in other *Second Life* blogs and websites. Information pointing out the problems associated with RedZone is available on hundreds of blogs, including a few such as *no2redzone* that are exclusively focused on the program. There are also videos that specifically address RedZone. In contrast, although there are blogs and webpages that make mention of programs like ChatSpy, even detailing their uses and how to avoid them, the information is more difficult to find, and is often focused on advertising and selling these programs rather than raising awareness of their implications for in-world interactions.

The extensive discussions on RedZone are partly motivated by the level of concern surrounding the technology. With the perceived anonymity and freedom of *Second Life*, IP addresses were seen as tethers back to offline life and to other online identities. As the program came into more widespread use, resident concern increased. The program's creator reported upwards of 17 000 sales ("Redzone's Scan Statistics" 2011), while marketplace data suggested that over 20 000 copies had been sold (Rhiadra 2011). Once participants recognized the scope of the application's in-world use and its potential for linking together identities, the threat to their second lives became more clearly defined. There is a marked difference between early forum threads from July 2010 and later coverage in February 2011. Earlier responses in forum threads commonly justify the use of RedZone or dismiss its efficacy ("ZF Redzone, Disclosure of SecondLife Alts" 2010). In contrast, later responses regularly discuss residents' concerns, especially in terms of the disclosure of IP addresses and alts, as well as tactics for dealing with the program ("Redzone: The WitchHunt.what's the REAL issue here?" 2011). Because RedZone relied on a database to store and compare information over time, it was also seen to potentially affect all *Second Life* residents who came into contact with it, either knowingly or unknowingly. With so many residents potentially affected by the program, discussions of the technology became not only commonplace, but also more focused on its implications and perceived threats.

Most other surveillance technologies rely on some resident involvement through their choice to use items like ChatSpy collars and what they do and say within the world (this, of course, does not imply that residents who reveal identifying or personal information while under surveillance are wrong for doing so, or are in any way deserving of the possible repercussions). In these examples, residents maintain some level of control over what information is available about them. In contrast, RedZone was seen to offer no such control because of its automatic detection of IP addresses without resident permission or awareness. As one resident explains:

There are ways to minimize your identification as an alt. I mean, duh, if you don't want that alt found, don't put information in that would obviously connect it to the primary. The problem is that tools like RZ are trying to *bypass* those common-sense measures, essentially saying that no matter what you do, your information is going to be shared. You don't even get to know about it or approve it, even. It's without your knowledge or consent" (Foxdale 2011).

Similarly, another states that, "RZ is a flat out invasion of privacy, you have no control over" (Himmel 2011).

Understanding and Awareness

The amount of information made available to *Second Life* residents about RedZone versus other surveillance technologies is useful in its own right, and indicates a high level of concern around this application and its potential repercussion. However, there are also differences in how these surveillance practices are discussed. Given the availability of RedZone information, confusion around the program is relatively rare. Its profile is high and information so abundant that although what poses the most pressing issue is debated, there are relatively few questions about its purpose and capacities. In addition, RedZone discussions often offer tactics to avoid or subvert the program, such as turning off streaming media (Kwong 2011).

Conversely, discussions around other technologies and their uses make evident that many residents are not as aware of their presence or capabilities. Posts that start threads about surveillance other than RedZone frequently begin with a question. One thread, for example, starts with a resident asking “I know trackers in SL are illegal. But what exactly do they do besides record conversations of a person who is on the other side of the sim. Do they also track IMs? Do they track you if you are off sim? I was told about them, but not in great detail. Can anyone help?” (Twine 2010). In this example, there is clear uncertainty about what exactly in-world surveillance can do. In the same forums another resident asks:

Today I was chatting with a friend on her land at the open channel and, even if no one was near 20 or 30 meters from us, she told me “There is someone spying on our chat...” ...I got intrigued: Is there a way you can tell if someone is spying on you? That chat listening is only for open chat or for private IM as well? To know you are being listened is because you are the land owner or for the use of an HUD [head’s up display, an application that overlays additional information onto the *Second Life* user interface] as well? And of course: can you block that action? (Guardian 2010)

In this instance, the resident has moved from no knowledge to some knowledge of surveillance; however, there is still recognizable confusion around what kind of surveillance is possible as well as its consequences and whether it can be avoided.

This example also points to another feature of discussions around in-world surveillance caused by lack of awareness. As in this example, much of the discussion of surveillance in *Second Life* is reactive rather than proactive or preventative. A common topic in the posted surveillance discussions are users who suspect that they are being watched or who have attached a device to their body that has done something that is usually unpleasant and unanticipated. These accounts are indicative of the willingness of some *Second Life* users to accept and use items that they are not necessarily familiar with, and their lack of awareness of the fact that these items may contain technologies that allow for surveillance. In the official *Second Life* forums, one resident tells the story of another resident who visits her club. She recounts:

The other day a regular visitor came to my club, and as I walked toward him to say hello his collar spammed my chat to tell me who owns him. This let me know it was one of those nasty creepy creepy little chatspy collars. I immediately switched to im. Turned out, he did not know his collar did that...did not know it was tracking all his teleports and reporting who is around him and what was said (Ember 2009).

The main issue in this account is the fact that user is unaware of what the collar he is wearing is capable of doing. Similar accounts appear in other *Second Life* discussions. In addition to having in-world movements and conversations recorded, residents detail being stalked or even controlled by other individuals (Giadelli 2010; Viper 2010) because they have used items that have built-in surveillance and

control. These accounts suggest that many residents are not aware of the possibilities for virtual surveillance or, in cases where help is requested, how to avoid or respond to it.

Perhaps even more telling is that in this example, the individual with the collar is described as a “regular visitor,” someone who has been in-world long enough to become known to a club owner, be referred to as a “regular,” and who is consequently not a newbie and likely not inexperienced. Despite presumably being at least somewhat familiar with the world, this resident is unaware enough of the possibility of surveillance that he attaches a piece of technology to his body, presumably without knowing what it is capable of or likely to do. As in this example, even residents who are somewhat established within the world can run into issues with surveillance when it is unanticipated.

Although residents may be aware of surveillance devices, they can also be unaware or skeptical of their efficacy. In a forum discussion, for instance, one resident dismisses the possibility of surveillance issues by saying “Shop owners often have objects for statistics on the traffic, for sending notecards or group invitations, don't feel paranoid, why would they spy your chat?” (Bode 2010). This disbelief is also captured in the words of Au, a long-time *Second Life* insider, and former official chronicler of the development of *Second Life* through the blog *New World Notes*. In looking into surveillance technologies, Au tries a bug designed for attaching to avatars and spying on conversations, and writes that:

Some bugs allow spies to hear conversations anywhere in the world, but Loki [Clifton] tells me that this particular bug he's put on me can only monitor nearby conversations on this island. I don't believe it, so I fly away from Loki Clifton and Biscuit Carroll, past 25 meters (beyond normal listening range), and keep flying until I'm hundreds of meters away. When I'm at the edge of the ocean, with no one around, I say something: “I'm wholly skeptical that this bug works.” I fly back to the building where Clifton and Carroll wait. “I'm wholly skeptical that this bug works,” Loki repeats back. “You can be as skeptical as you like, Hamlet,” Biscuit Carroll tells me. “The effing thing works” (Au 2007).

Despite his long tenure as a *Second Life* insider, Au reveals disbelief and skepticism with regards to the functionality of the technology. These sentiments are echoed in online discussions, both in residents' uncertainty about what surveillance is capable of and a general disbelief that surveillance is possible and does what they have been told it can do. In believing that these technologies may not work, residents are at a disadvantage, especially if they do not seek to protect themselves from such intrusions.

Surveillance and the Socio-Technical Environment

There is a marked contrast between the discussions of RedZone and other surveillance technologies, both in terms of amount of discussion and the ways in which these technologies are approached. Participant concerns are largely responsible for the significant amounts of attention paid to RedZone. The importance of these concerns as a driving force behind awareness and discussion is evident when compared with other technologies that are not as frequently debated due to less widespread use, less of a perceived threat, and a greater sense of control. However, there are also other factors that work to conceal and downplay the presence of these technologies and their uses. The technological and social constructions of the world function in ways that not only make surveillance possible, but that also obscure the presence and potential consequences of many surveillance practices.

In a practical way, surveillance in *Second Life* is made possible by the prevalence and necessity of user-generated content. Whereas other virtual environments such as those in video games are tightly controlled in order to maintain an even playing field (Castronova 2005), *Second Life* relies almost exclusively on what users create. While this work provides much of the world's content, it also makes it possible for

residents to build and deploy surveillance technologies that can be used to monitor, track, and record other residents, often in ways that are hidden, if not invisible. With its reliance on user-generated content, *Second Life* allows for a form of lateral surveillance that enables individual to use technologies and applications on each other, rather than being strictly the preview of institutions (Andrejevic 2005).

Surveillance is also facilitated by the technical affordances of *Second Life* that are made use of by content creators. RedZone, for instance, exploited *Second Life*'s media streaming capabilities that allowed music and videos to be played within the world. When a resident came in range of the program, it caused the resident's computer to access a website, allowing their IP address to be revealed and recorded. Other technologies make use of the digital nature of in-world surveillance to conceal technologies in other items, such as lamps or vases, or to make them extremely small visually, in some cases only a pixel large. In these instances, surveillance can be difficult to detect, and therefore difficult for residents to guard against.

Other elements that help to downplay the potential for and role of in-world surveillance are the ways in which surveillance technologies are positioned, both within the world and in terms of sales and related discussions, and the amount of information that they collect. For the former, many of the technologies used in surveillance are similar if not identical to technologies that are used in more recognized and less insidious ways. For instance, greeter technologies are frequently used in *Second Life*, especially in public and commercial sims. The technology that surreptitiously tracks what residents have visited a particular sim and when is very similar to the technology that is used to greet visitors and offer them information about an area to which they have teleported.

Because technologies that are used innocuously are very similar, if not identical to those used for surveillance, it can be difficult to determine whether the program is used only to greet residents or whether it is being used as a tool of surveillance. Participants, however, are accustomed to being greeted by these programs, since they are used throughout *Second Life*. Given their commonplace presence and their helpful purpose, these technologies not only appear to be innocuous, but also helpful. Studies suggest that people are often willing to give up their personal information in order to obtain something that they want (Milne and Gordon 1993; Hafner 2006; Fischer 2001). The fact that surveillance technologies often appear in ways that are helpful in *Second Life* increases the chance that residents will be willing to give up information or will not suspect problematic motives.

Surveillance technologies available in-world and through the *Second Life* marketplace are described by proponents largely in terms that make them sound relatively harmless. For instance, one program is advertised as "A sensor to greet and record the names of visitors and their arrival time" (Melendez 2011), a description that is more reminiscent of a greeter and guest book than tracking software. The implications of these technologies are also downplayed by the seemingly limited amount of information collected and the context in which it is gathered. While this technology represents relatively small amounts of information—avatar names and arrival times, for instance—it is still collecting information. Scholars have suggested that,

A particular piece of data about you—such as the fact that you entered your office at 10:29 am on July 2, 2001—is normally innocuous. But when enough pieces of that kind of data are assembled together, they add up to an extremely detailed and intrusive picture of an individual's life and habits (Stanley and Steinhardt 2009).

The fact that these technologies record what appear to be relatively small amounts of information, and information that is not linked to other avatars or the offline self, downplays the presence of in-world surveillance. Even though some information can be perceived as innocuous, but becomes invasive when taken out of context (Adams and Sasse 1999).

The perception of surveillance technologies as innocuous is also facilitated by how such technologies are described and justified. Of those ads that do advertise their actual and potentially more suspect uses, many position the technology in terms of blaming other participants for their necessity. One ad claims, for example, that “it's a great way of finding out who has been snooping around you're [sic] home or business while you're not there” (Zapedzki 2011). In this instance, while the purpose of the technology is made clear in no uncertain terms, it is positioned in a way that suggests that using surveillance measures is, at least in some instances, necessary and justified. Eye-Spy Security & Surveillance advertises that, “Whether you need to protect your Land from unwanted visitors, or own/manage a large SIM, we have everything you need” (*Eye-Spy Security & Surveillance* 2011). With a focus on protection and management, surveillance is positioned as necessary and justifiable, rather than something that could be used in less acceptable ways.

Finally, the presence of surveillance is also obscured by the fact that the amount of surveillance and who is using it is difficult to track, since technologies can be built or used by any resident with the requisite technical skills. There are few measures that indicate exactly how much surveillance is in use and to what ends. Because surveillance is user-created and deployed, official figures are not available. Although the reviews of some surveillance systems suggest that they are being purchased and used, neither the marketplace nor in-world sales sites account for exactly how many of a particular item has been sold. Furthermore, the marketplace does not account for user-created systems, in-world sales, or other one-to-one sales between residents. As such, it is almost impossible for residents to determine to what extent surveillance is being used within the world, and by whom.

Collectively, these technological and social facets of the virtual world work to obscure the presence and effects of different forms of in-world surveillance. Although RedZone has gained notoriety among *Second Life* residents, the same levels of discussion, information, and awareness are not commonly found about other programs that present similar threats to in-world and offline privacy. While they do not present the same immediate threat as is felt in relation to the use of IP addresses in surveillance, they also remain hidden by the technical affordances of the world as well as the ways that surveillance is used, positioned, and justified within it.

Resistance

Although it is the socio-technical environment that enables surveillance, it also makes resistance possible. When participants are aware of surveillance they can raise awareness in others, change their behaviours within the world, develop ways of circumventing the technologies, and even alter the behaviour of others. Although rarely seen with other surveillance practices, the perceived threat of RedZone caused a large swell of discussions that helped raise participant awareness through forums, blogs, wikis, and other web-based *Second Life* sites that allowed for user-generated content and user comments.

Increased awareness, in turn, allowed participants to respond to the program if they deemed it a threat to their virtual or offline lives. For instance, when RedZone was recognized as an issue, awareness of its use allowed residents to stay away from areas that were using the technology. Some residents opted to disable the in-world media streaming that allowed RedZone to detect IP addresses (Samael 2011) while some relied on proxy servers and programs to hide their IP address (Alex 2011). Others found ways to detect the technology, with some avoiding RedZone sims and the owners that used the program, and others seeking to start boycotts (Magic 2011).

Just as user-generated content and the technical affordances of the world can be used to develop surveillance technologies, so too can they be used in counter-surveillance efforts. Combatting RedZone was also facilitated by the development of GreenZone, a program designed to detect the program and

identify where it was being used in-world. This information was made public, and used as leverage to try to convince residents who were using RedZone to stop. The anti-RedZone lobby was used to successfully pressure in-world business and land owners to not use the technology on their land. In one such discussion a participant writes that:

Those who have used this thing—I hate to sound like McCarthy here—but I don't intend to throw any business your way until you have made some sort of statement to your customers that you did not understand what this thing really does to people, and that you have removed it, and will not use it in the future (Magic 2011).

Eventually the pressure became so great that Linden Lab banned the program's creator from *Second Life* and removed the program itself from the marketplace and in-world stores. At the same time, they also amended *Second Life*'s Community Standards to state:

Residents are entitled to a reasonable level of privacy with regard to their *Second Life* experience. Sharing personal information about your fellow Residents without their consent—including gender, religion, age, marital status, race, sexual preference, alternate account names, and real-world location beyond what is provided by them in their Resident profile—is not allowed. ("Community Standards" 2011)

While these standards do require that residents not make any details that can be gleaned from this information public, they do not explicitly ban the tracking of IP addresses or any other form of surveillance.

As shown in the response to RedZone, there are many ways to deal with the threat of in-world surveillance, from avoiding areas that engage in surveillance to turning off in-world media, and from raising awareness to engaging in counter-measures. Although the technical agency available within *Second Life* makes surveillance possible in myriad and often difficult to detect ways, it also makes possible a number of different options for resisting these practices, especially when they are an intrusion into online or offline life. These responses, however, depend on residents being aware of the possibility of being subject to surveillance and knowing what they can do to address it, which is not always facilitated within *Second Life*.

Conclusions

It would be relatively easy to suggest that surveillance is not an issue in *Second Life*. RedZone, the technology that tracks IP addresses and is perceived to pose the biggest threat, has been at least partially dealt with by resident protest. The RedZone case, therefore, not only demonstrates the possibilities for surveillance in *Second Life*, but also the ways in which concerned residents can resist. However, as much as RedZone presents what is perhaps an ideal example of recognizing, discussing, and dealing with surveillance, it remains that there are still issues with surveillance practices in the virtual world. Given *Second Life*'s socio-technical environment, other forms of surveillance are often hidden, obscured, or presented in ways that downplay the potential implications for virtual and offline life.

Speaking to the modern culture of surveillance, Lyon asserts that, "people seldom know that they are subjects of surveillance, or, if they do know, they are unaware how comprehensive others' knowledge of them actually is" (1994, 5). This idea is echoed by a *Second Life* resident who recommends that "All users of SL should be aware that tiny, invisible objects might be relaying their conversations to other AVs, or even sending IMs or HTTP messages out of SL. A bit like real life really, it's just that bugging is easier in SL" (sparti 2007). While RedZone is a program that residents are very aware of, other forms of

surveillance in use in-world make it difficult, as Lyons claims, to be fully aware of what surveillance is taking place, as well as what information other people are able to gather and how they are using it.

In some ways, *Second Life* surveillance is similar to that seen in offline life and other online media. Although not necessarily as prevalent or as linked to bureaucracy, it does serve as a form of social control (Campbell and Carlson 2002). This is especially true in the case of RedZone, where the program is used to prevent grievers or CopyBot users from entering particular sims, and to dissuade other residents from likewise causing trouble.

The effects of these intrusions, however, are different. Although they happen within a virtual world, the consequences of *Second Life* surveillance can pose significant problems for residents. *Second Life* is perceived to offer the privacy that everyday life often does not. Furthermore, because of the anonymity and the freedom of the world, online interaction can be a powerful experience for residents who use the virtual space. For those who value their virtual life or lives for exploration, adventure, identity play, or simply trying new things, links made between avatars or to offline identities threaten to disrupt the security of online life and to expose information, activities, and preferences that they wish to maintain as hidden or separate from particular identities.

Speaking to surveillance, a resident suggests to others that, “If you are overly concerned about privacy, then SL is the wroooooong place” (Avedon 2010). In one sense, they are correct. The virtual world and the ways that surveillance is presented within it make it difficult to gain a complete understanding of the presence, use, and implications of surveillance. In turn, maintaining in-world privacy can be a difficult task, and one that is not engaged by all residents for a variety of reasons ranging from not seeing the technology as a threat to being unaware of in-world surveillance. Viewed through another lens, however, it is also apparent how *Second Life* also creates a virtual space in which surveillance can be detected, discussed, and even addressed by the very participants whom it affects. Although there are issues with the presence of surveillance in *Second Life* and the ramifications of these technologies, it remains that the virtual world also offers a variety of approaches to deal with any threats, impositions, or issues posed by such practices.

References

- Adams, Anne, and M. Angela Sasse. 1999. “Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs, or Let Them Lie?” Paper presented at HCI - Interact '99, Edinburgh, Scotland, August 30-September 3.
- Alex. 2011. “RedZone, Second Life IP Address Detection Tool, Runs Afoul of New SL Policy, EU Data Privacy Law.” *Virtual Navigator*, February 28. Retrieved from <http://virtualnavigator.wordpress.com/2011/02/28/redzone-second-life-ip-address-detection-tool-runs-afoul-of-new-sl-policy-eu-data-privacy-law/>.
- Andrejevic, Mark. 2005. “The work of watching one another: Lateral surveillance, risk, and governance.” *Surveillance & Society* 2 (4):479–497.
- Au, Wagner James. 2007. “Spy game.” *New World Notes*, February 13. Retrieved from http://nwn.blogs.com/nwn/2007/02/spy_game.html.
- Au, Wagner James. 2011. “How Widespread is the Redzone IP Tracking Controversy in Second Life? (UPDATED).” *New World Notes*, February 13. Retrieved from <http://nwn.blogs.com/nwn/2011/02/redzone-ip-controversy-second-life.html>.
- Avedon, Santirix. 2010. “Usage of Chat-Spy Radar—Legitimate, or Spying Only?” *Second Life Forums*, August 9. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Usage-of-Chat-Spy-Radar-Legitimate-or-Spying-Only/m-p/310881/highlight/true-M126308>.
- Bardzell, Jeffrey, and Shaowen Barzell. 2006. “Sex-Interface-Aesthetics: The Docile Avatars and Embodied Pixels of Second Life BDSM.” *Proceedings of the Conference on Human Factors in Computing Systems*, Montreal, Quebec, Canada, April 24–27.
- Bargh, John A., Katelyn Y.A. McKenna and Grainne M. Fitzsimons. 2002. “Can you see the real me? Activation and expression of the ‘true self’ on the Internet.” *Journal of Social Issues* 58 (1):33–48.
- Barnes, Wayne R. 2005. “Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance.” *UC Davis Law Review* 39.
- Blinka, Lukas. 2008. “The Relationship of Players to Their Avatars in MMORPGs: Differences between Adolescents, Emerging Adults and Adults.” *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 2 (1).

- Bode, herina. 2010. "Spying on chats?" *Second Life Forums Archive*, August 8. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Spying-on-chats/td-p/309088>.
- Brookey, Robert Alan, and Kristopher L. Cannon. 2009. "Sex Lives in Second Life." *Critical Studies in Media Communication* 26 (2):145-164.
- Bugeja, Michael J. 2007. "Second Thoughts About Second Life." *The Chronicle of Higher Education* (September 14, 2007).
- Campbell, John Edward, and Matt Carlson. 2002. "Panopticon.com: Online Surveillance and the Commodification of Privacy." *Journal of Broadcasting & Electronic Media* 46 (4):506-606.
- Castronova, Edward. 2005. *Synthetic Worlds: The Business and Culture of Online Games*. Chicago: University of Chicago Press.
- "Community Standards." 2011. Retrieved from <http://secondlife.com/corporate/cs.php>.
- Dudley, Alfreda, James Braman, Yuanqiong Wang, Giovanni Vincenti, and Donna Tupper. 2010. "Security, Legal, and Ethical Implications of Using Virtual Worlds." Paper read at Systemics, Cybernetics and Informatics: WMSCI 2010 June 29 to July 2, at Orlando, Florida, USA.
- Ember, Succubus. 2009. "Banning Chat Spy Collars?" *Second Life Forums*, March 9. Retrieved from <http://community.secondlife.com/t5/Blogs/ct-p/Blogs>.
- Eye-Spy Security & Surveillance*. 2011. Accessed December 26, 2011. <http://world.secondlife.com/group/261eef55-7390-5209-c04a-2f9fccc71d24>.
- Fischer, Susanna Frederick. 2001. "Saving Rosencrantz and Guildenstern in a Virtual World—A Comparative Look at Recent Global Electronic Signature Legislation." *Journal of Science & Technology Law* 7.
- Flaherty, David H. 1992. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC: UNC Press.
- Foxdale, Relm. 2011. "Redzone: The WitchHunt.what's the REAL issue here?" *Second Life Forums*, February 18. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Redzone-The-WitchHunt-what-s-the-REAL-issue-here/td-p/517275>.
- Gandy, Oscar H., Jr. 2006. "The Surveillance Society: Information Technology and Bureaucratic Social Control." *Journal of Communication* 39 (3):61-76.
- Giadelli, Faith. 2010. "Chat spy and other interesting gadgets." *Second Life Forums*, August 9. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Chat-spy-and-other-interesting-gadgets/m-p/310721/highlight/true-M126232>.
- Guardian, Warlock. 2010. "Spying on chats?" *Second Life Forums*, August 8. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Spying-on-chats/m-p/309088/highlight/true-M125381>.
- Hafner, Katie. 2006. "After Subpoenas, Internet Searches Give Some Pause." *New York Times*, January 25. Retrieved from http://www.nytimes.com/2006/01/25/national/25privacy.html?_r=1&pagewanted=1&ei=5094&en=53ada0c511b528d5&hp&ex=1138165200&partner=homepage.
- Himmel, Norsk. 2011. "Why is Redzone allowed?" *Second Life Forums*, February 2. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Why-is-Redzone-allowed/td-p/376815/page/8>.
- Kafai, Yasmin B., Deborah A. Fields, and Melissa S Cook. 2010. "Your Second Selves: Player Designed Avatars." *Games and Culture* 5 (1):23-42.
- Kuramoto, Masami. 2011. "How Widespread is the Redzone IP Tracking Controversy in Second Life? (UPDATED)." *New World Notes*, February 13. Retrieved from <http://nwn.blogs.com/nwn/2011/02/redzone-ip-controversy-second-life.html>.
- Kwong, Justin. 2011. "RedZone, Second Life IP Address Detection Tool, Runs Afoul of New SL Policy, EU Data Privacy Law." *Virtual Navigator*, February 28. Retrieved from <http://virtualnavigator.wordpress.com/2011/02/28/redzone-second-life-ip-address-detection-tool-runs-afoul-of-new-sl-policy-eu-data-privacy-law/>.
- Lili. 2011. "How Widespread is the Redzone IP Tracking Controversy in Second Life? (UPDATED)." *New World Notes*, February 13. Retrieved from <http://nwn.blogs.com/nwn/2011/02/redzone-ip-controversy-second-life.html>.
- Linden Lab. 2011. "The Second Life Economy in Q3 2011." *Second Life Blogs*, October 14. Retrieved from <http://community.secondlife.com/t5/Featured-News/The-Second-Life-Economy-in-Q3-2011/ba-p/1166705>.
- Llewelyn, Gwyneth. 2009. "The Hard Facts About the Second Life Economy" *Gwyn's Home*, October 13. Retrieved from <http://gwynethllewelyn.net/2008/10/13/the-hard-facts-about-the-second-life-economy/>.
- Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
- Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. In *Issues in Society*, ed. T. May. Philadelphia, PA: Open University Press.
- Magic, Mileta. 2011. "RedZone users - *Please Ban Me*." *Second Life Forums*, February 12. Retrieved from <http://community.secondlife.com/t5/General-Discussions/RedZone-users-Please-Ban-Me/m-p/508747/highlight/true-M249975>.
- Magic, Theia. 2011. "Redzone: The WitchHunt.what's the REAL issue here?" *Second Life Forums*, February 18. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Redzone-The-WitchHunt-what-s-the-REAL-issue-here/td-p/517275>.
- Makkai, Toni. 2009. "The future of technology-enabled crime in Australia." *Trends and Issues in Crime and Criminal Justice* 341. Retrieved from <http://www.aic.gov.au/publications/current%20series/tandi/341-360/tandi341/view%20paper.aspx>.
- McKenna, Katelyn, Amie Green, and Marci Gleason. 2002. "Relationship Formation on the Internet: What's the Big Attraction?" *Journal of Social Issues* 58 (1):9-31.

- McMasters, Madelaine. 2011. "Redzone: The WitchHunt.what's the REAL issue here?" *Second Life Forums*, February 18. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Redzone-The-WitchHunt-what-s-the-REAL-issue-here/td-p/517275/page/2>.
- McMasters, Madelaine. 2011. "Redzone: The WitchHunt.what's the REAL issue here?" *Second Life Forums*, February 18. Retrieved from <http://secondlife.lithium.com/t5/General-Discussions/Redzone-The-WitchHunt-what-s-the-REAL-issue-here/td-p/517275>.
- Melendez, Jon. 2011. "Surveillance sensor and greeter." *Second Life Marketplace*. Retrieved from <https://marketplace.secondlife.com/p/Surveillance-sensor-and-greeter/370314>.
- Milne, George R., and Mary Ellen Gordon. 1993. "Direct Mail Privacy—Efficiency Trade-Offs Within an Implied Social Contract Framework." *Journal of Public Policy & Marketing* 12 (Fall): 206-215.
- Norris, C., and G. Armstrong. 1999. *The Maximum Surveillance Society: The rise of CCTV*. Oxford: Berg.
- Obscure, Opensource. 2011. "How Widespread is the Redzone IP Tracking Controversy in Second Life? (UPDATED)." *New World Notes*, February 13. Retrieved from <http://nwn.blogs.com/nwn/2011/02/redzone-ip-controversy-second-life.html>.
- Propen, Amy D. 2006. "Critical GPS: Toward a New Politics of Location." *ACME: An International E-Journal for Critical Geographies* 4 (1):131-144.
- Reahard, Jef. 2011. *Habbo Hotel touts 200 million registrations*. Joystiq. Retrieved from <http://massively.joystiq.com/2011/02/03/habbo-hotel-touts-200-million-registrations/>
- "Redzone: The WitchHunt.what's the REAL issue here?" 2011. *Second Life Forums*, February 18. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Redzone-The-WitchHunt-what-s-the-REAL-issue-here/td-p/517275>.
- "Redzone's Scan Statistics." 2011. *no2redzone*, February 7. Retrieved from <http://no2redzone.wordpress.com/2011/02/07/how-many-redzone-sites-are-there/>.
- Rhiadra, Scylla. 2011. "'Speak to Me Your Song of Greed': Redzone and the Economics of Fear." *Second Life Left Unity*, February 22. Retrieved from 2012. <http://slleftunity.blogspot.ca/2011/02/speak-to-me-your-song-of-greed-redzone.html>.
- Samael. 2011. "RedZone, Second Life IP Address Detection Tool, Runs Afoul of New SL Policy, EU Data Privacy Law." *Virtual Navigator*, February 28. Retrieved from <http://virtualnavigator.wordpress.com/2011/02/28/redzone-second-life-ip-address-detection-tool-runs-afoul-of-new-sl-policy-eu-data-privacy-law/>.
- Shapiro, Brian and C. Richard Baker. 2001. "Information technology and the social construction of information privacy." *Journal of Accounting and Public Policy* 20: 295-322.
- Slobogin, Christopher. 2002. "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity." *Mississippi Law Journal* 72.
- Slobogin, Christopher. 2007. *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*. Chicago, IL: University of Chicago Press.
- Slot, Mijke. 2009. "Exploring user-producer interaction in an online community: the case of Habbo Hotel." *International Journal of Web Based Communities* 5 (1):33-48.
- Smith, Justin. 2011. "Inside Virtual Goods: Tracking the US Virtual Goods Market 2011—2012, Is Here." *Inside Facebook*, December 6. Retrieved from <http://www.insidefacebook.com/2011/12/06/inside-virtual-goods-tracking-the-us-virtual-goods-market-2011-%E2%80%93-2012-is-here/>.
- sparti. 2007. "Mission Spy—it spies on other AVs." *Second Life Wiki*. Retrieved from <http://www.sparticarroll.com/Mission+Spy.ashx>.
- Stanley, Jay, and Barry Steinhardt, eds. 2009. *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society. Readings in the Philosophy of Technology*, ed. D. M. Kaplan. Lanham, MD: Rowman & Littlefield Publishers, Inc.
- Stillwagon, Bryan Andrew. 2007-2008. "Bringing an End to Warrantless Cell Phone Searches." 42 *Ga. L. Rev.* 1165.
- Taylor, Marisa. 2009. "Your Second Life Avatar is Dressed Inappropriately." *Digits: The Wall Street Journal*, October 9. Retrieved from <http://blogs.wsj.com/digits/2009/10/09/your-second-life-avatar-is-dressed-inappropriately/>.
- Turkle, Sherry. 1995. *Life on the Screen: Identity in the Age of the Internet*. New York, NY: Simon and Schuster.
- Twine, Melrose. 2010. "Trackers..." *Second Life Forums*, September 5. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Trackers/m-p/348275/highlight/true-M151696>.
- Viper, Seductress. 2010. "Can't log on because *he's* there!" *Second Life Forums*, June 6. Retrieved from <http://community.secondlife.com/t5/General-Discussions/Can-t-log-on-because-he-s-there/m-p/228282/highlight/true-M74921>.
- Wolfendale, Jessica. 2007. "My Avatar, My Self: Virtual Harm and Attachment." *Ethics and Information Technology* 9 (2):111-119.
- Zapedzki, Supersshine. 2011. "Tracking Security Camera CCTV Security System Video Surveillance Cameras." *Second Life Marketplace*. Retrieved from <https://marketplace.secondlife.com/p/Tracking-Security-Camera-CCTV-Security-System-Video-Surveillance-Cameras/916053>.
- "ZF Redzone, Disclosure of SecondLife Alts." 2010. *SLUniverse*, July 30. Retrieved from <http://www.sluniverse.com/php/vb/general-sl-discussion/47314-zf-redzone-disclosure-secondlife-alt.html>.