Surveillance & Society

Article

Deviance and Control in Communities with Perfect Surveillance – The Case of Second Life

Victoria Wang

Department of Computer Science, College of Science and Centre for Criminal Justice and Criminology, School of Law, Swansea University, Swansea SA2 8PP, UK. csvic@swansea.ac.uk; vichil471026@hotmail.com

Kevin Haines

Centre for Criminal Justice and Criminology, School of Law, Swansea University, Swansea SA2 8PP, UK. k.r.haines@swansea.ac.uk

John V. Tucker

Department of Computer Science, College of Science, Swansea University, Swansea SA2 8PP, UK. j.v.tucker@swansea.ac.uk

Abstract

Advanced cybercommunities are communities in which perfect surveillance is possible – software tools allow everything to be observed, recorded, archived, pored over at a later date and acted upon. Hence, one expects that these surveillance technologies ought to be heavily used and effective in controlling deviance in these cybercommunities. Drawing on our research in the cybercommunity Second Life, we observe that surveillance technologies are not heavily used to deal with deviance; instead, it is the power of relationships that form the fabric of social control and the regulation of deviance. This discovery questions the effectiveness of technology as a regulator, both in Second Life and in the real world, as well as evidences the importance of social bond as a mediator of deviance.

Key Words: deviance, surveillance technology, cybercommunities, control, social bond

Introduction

It seems that building a surveillance society is the means to achieve a secure society (Lyon 2007). The building of a surveillance society has generated a new security architecture – increasingly, surveillance technologies and techniques are built into our physical and virtual surroundings, and surveillance practices are increasingly becoming an inseparable part of our everyday life (Jones 2005; Lyon 2007; Zedner 2009). In particular, the significant growth in surveillance technologies in policing and related functions seems to be sending a general message – surveillance is good for society and technology is the source of our security.

Wang, Victoria; Haines, Kevin; Tucker, John V. 2011. Deviance and Control in Communities with Perfect Surveillance – The Case of Second Life. *Surveillance & Society* 9(1/2): 31-46.
http://www.surveillance-and-society.org | ISSN: 1477-7487

The growth in surveillance technologies in both number and application is taking place in the face of a continuous debate over the lack of effectiveness, high financial cost and negative social consequences of these technologies (e.g. Lyon 1994; Norris and Armstrong 1999; Armitage 2002; McCahill 2002; Welsh and Farrington 2008; Coleman and McCahill 2011). Yet, the fallibility and failure of surveillance technologies lead not to their abandonment, but to an approach that attributes the lack of effectiveness to insufficient numbers, applications and coverage of these technologies. For example, over a decade ago, in their observational study of the open-street CCTV surveillance cameras, Norris and Armstrong (1999) showed how the operation of these systems "rather than contributing to social justice through the reduction of victimisation ... may become a tool of injustice through the amplification of differential and discriminatory policing" (ibid: 201). This discovery and others (e.g. Goodwin 2002; Griffiths 2003; Gill and Spriggs 2005; Gill et al. 2006; Farrington et al. 2007; Woodhouse 2010) have led to a counterfactual proliferation of 'automated socio-technical systems', such as further applications of CCTV surveillance systems (e.g. CCTV speed cameras that target 'respectable citizens' (Finn and McCahill 2010)), to watch "more people from more walks of life" (Haggerty and Ericson 2006: 5) and to eventually lead to a 'non-discriminatory' rationale for monitoring by targeting the entire population (Lianos and Douglas 2000). Despite the empirical evidence, it seems that the faith in surveillance technologies as effective mechanisms of promoting and achieving a secure society is unshakeable. Following this belief, surveillance technologies should work at their best in an environment where these technologies are ubiquitous, i.e. where there is complete technological surveillance or *perfect surveillance*, such as one finds in certain cybercommunities.

The cybercommunity Second Life is an environment where perfect surveillance is endemic to the environment. Second Life was created to replicate, reflect, extend and expand the real world, and therefore contains features common to many contemporary societies, cultures and all kinds of advanced human activities. Thus, sociologically, Second Life is an authentic social community with a rich communal life, including deviance. Technologically, however, it is a piece of computer software – its functions and limitations are determined by the programmers who design and build the system architecture. Thus, it is perfectly possible for the programmers to build automated systems which carry out actions that prevent, confront or punish deviant behaviour at any time, with no need for human input and no room for subjects to negotiate with the surveillance regime. Actually, Second Life is a place where 'dataveillance' (van der Ploeg 2003: 71) is endemic – every word typed by the residents and every movement made by their virtual bodies can be observed, recorded, stored in digital files and pored over in real time or later over long time intervals. In this way, Second Life is a true automated socio-technical environment – an extreme exemplar of many automated socio-technical environments constructed by tracking devices, machine-based access control, automated CCTV, and so on, in the real world (cf. Lianos and Douglas 2000). In the cybercommunity, it is possible to use "No other logic than whatever is programmed into [its] software whereby access is accepted or denied; identity is either confirmed or rejected; behaviour is either legitimate or illegitimate" (Norris 2003: 276). Indeed, Second Life can create and sustain a totalitarian cyber state that is equal to anything found in science fiction – even in the work of the bleakest imagination building on George Orwell's *Nineteen Eighty-Four* (1948).

In short, Second Life is home to thousands of communities in which perfect surveillance is practically possible and easily achievable. In this context, therefore, one might reasonably expect that surveillance technology be heavily used to regulate deviance in the cybercommunity. Moreover, if surveillance technology works as an effective regulator, then it should work at its best in Second Life, where the environment is constructed by technologies, where technology is native to its social life – all activities, including the deviant ones, are carried out in full three dimensional (3D) detail, through technological tools, where 'absolute security is no longer a chimera' (Zedner 2003: 158).

In this article, we draw on our research on deviance that was carried out in the cybercommunity Second Life. Our empirical research consisted of participant observation, survey research and discussion in a

Second Life residential forum (Wang 2009). Following participant observation, a standard list of 91 acts covering different types of potentially deviant acts and a list of 39 motivations for becoming residents of Second Life were constructed and translated into three different questionnaires (Wang 2009). These questionnaires were sent to three different samples of participants in Second Life to assess individual participants' perception, experience and performance of deviance in the cybercommunity. In the first questionnaire, the participants were asked to provide information about their perception of each of the 91 deviant acts[1] and to rate the extent of their motivation for participation in Second Life by each of the 39 motivations.[2] In the second and third questionnaire, the participants were asked to provide information about the number of times that they had experienced or performed each of the 91 potentially deviant acts, during their last ten substantial[3] visits in Second Life.[4] A thematic list of 16 questions focusing on the key themes that had emerged from the survey research was formulated based on the data derived from the questionnaires (Wang 2009). These questions were posted on a Second Life residential forum named *Resident Answers* over a period of 96 hours, with the purpose of initiating and stimulating discussion and debate about the nature and regulation of deviance among participants in Second Life – generating rich qualitative data.

Our findings suggest that deviance is not the dominant culture of Second Life. Instead the normal disciplines by which individuals act and evaluate acts in the real world are strongly evident in the cybercommunity. This finding is in contrast to the existing academic view which suggests that some fundamental characteristics of cybercommunities are responsible for high levels of deviance (e.g. Presdee 2000; Williams 2003, 2006, 2007; Wall 2007), as well as the media portrayal of the 'dark side' of Second Life encouraging the idea that cybercommunities are 'hotbeds of deviance' (Holahan 2006).

This does not mean that there is no notion of deviant behaviour or an absence of deviance in Second Life. Our findings show that acts that are considered as highly deviant are technology-related and may only be carried out by individuals with advanced technical skill (e.g. "using programs to take over another avatar" and "using programs to vandalise community property"). After these, there are acts that are child-related (e.g. "exchanging child related pornographic material" and "an adult using Teen Second Life to make contact with young adults for sexual purposes"). Then, there are acts that damage and disrupt Second Life as a community (e.g. "actions that are designed to slow down Second Life server performance" and "actions that diminish the Second Life community as a whole"). These are followed by a wide range of acts that contravene the *Big Six*[5] and other established institutional and local norms in Second Life, as well as many text and graphic related acts (e.g. "revealing the real life identity of another avatar" and "sending harassing Instant Message (IM) to another avatar"). Lastly, there are acts that can be considered as more extreme expressions of many liberal ideas that already exist in the real world (e.g. "a married individual marrying another avatar in Second Life" and "using a threatening or aggressive looking avatar"). Overall, however, one of the more surprising and relevant findings of our research is the relatively low level of deviance and victimisation reported by participants in Second Life. Our data shows that more than 70%, and more than 85%, of our questionnaire respondents reported that they had never experienced, or performed, any of the acts on the standard list, respectively.

[1] They were to select one of the five response categories: 1 = Not at all deviant; 2 = Slightly deviant; 3 = Certainly deviant; 4 = Very deviant; and 5 = Don't know.

[2] They were to select one of the five response categories: 1 = Not at all motivated; 2 = Not very much motivated; 3 = A bit motivated; 4 = Quite a lot motivated; and 5 = Very much motivated.

[3] Each of those visits lasting longer than an hour.

[4] They were to select one of the five response categories: 1 = 0 times; 2 = 1-5 times; 3 = 6-10 times; 4 = 11- 15 times; and 5 = more than 15 times.

[5] On an institutional level, Linden Lab sets out six kinds of major 'crime' in Second Life, which include 'intolerance', 'harassment', 'assault', 'disclosure', 'adult regions, groups, and listings' and 'disturbing the peace' (see: http://secondlife.com/corporate/cs.php; accessed 04/08/2011).

More importantly, the apparently low frequency of deviance in Second Life was not attributed to any formal surveillance carried out by Linden Lab using technological tools. Our participants, it seems, were either unaware or unconcerned by the extreme possibilities for surveillance. Actually, our data suggests that the 'state' – the creator of the Second Life software, Linden Lab – appears very reluctant to use the technological tools at its disposal to regulate deviance. This reluctance is conspicuously antithetical to the technological capability of Second Life. Moreover, the panoply and power of technological surveillance and regulation that are available to Linden Lab are not fully accessible to proxies in the cybercommunity. Proxies – what one may think of as organic local governments – have limited power to use technological tools to punish, but they can monitor and record online behaviour. Thus, because of the technological nature of the environment, proxies are able to exercise technological regulation.

Consequently, a question arises: *Why do individuals obey the rules and norms in Second Life?* Drawing on empirical data, our analyses of personal and social bonds between individuals and the Second Life community, and between individuals in communities in Second Life reveal that it is the power of relationships that form the fabric of social control and the regulator of deviance. Thus, our data sheds a new light on the heavy adoption of surveillance technology in policing and related functions. Drawing on the data, we challenge the very idea of using technology as a regulator, and the effectiveness of technology as a regulator, in controlling and regulating deviance, both in Second Life and in the real world.

On Second Life and Deviance in the Cybercommunity

Our empirical field of enquiry – the cybercommunity Second Life – is a 3D Internet-based cybercommunity developed by Linden Lab. It was first launched to the public on June 23, 2003. Anyone can become a resident of Second Life by downloading a client program named *Second Life Viewer* and interacting with other residents via self-created 3D avatars (Carr and Pond 2007). Actually, user-created content is the fundamental feature of Second Life. At its inception, the chairman of Linden Lab, Philipp Rosedale, wanted to design a virtual world where there is no barrier between thought and action (Guest 2007). With that vision in mind, Linden Lab only developed the virtual physics, designed the interface, invented the basic rules covering ownership and hoped that a society would emerge (Rymaszewski et al. 2007). A society has, indeed, emerged – practically it is built by its residents using a programming language named Linden Scripting Language (LSL) (Boellstorff 2008). Second Life has grown into the most popular international cybercommunity, which consists of thousands of user-defined sub-communities and groups with an extensive range of themes and purposes, such as business, entertainment, education, leisure, etc. (Carr and Pond 2007).

In particular, the real-world tradability of Linden Dollars (L$) (the currency in Second Life) has made real estate the most lucrative activity in Second Life, and has – in the most tangible way – connected the cybercommunity and the real world. For example, in November 2006, Anshe Chung declared herself Second Life's first millionaire in US dollars.[6] In 2007, Linden Lab estimated that Chung made US$150,000 per year from buying and selling virtual lands in Second Life (Rymaszewski et al. 2007). Besides business entrepreneurs, other groups of individuals, such as writers, musicians, politicians and academics, have joined Second Life, to reach a new audience, to experiment with a synthetic universe, or to have a taste of an innovative way of communication. For example, the realm of academia is represented by the cyberspace law expert – Lawrence Lessig; the man who first introduced and defined the term 'virtual community' – Howard Rheingold; and the man whose novel *Snow Crash* (1992) inspired the creation of Second Life – Neal Stephenson.

[6] See: http://www.businessweek.com/magazine/content/06_18/b3982002.htm (accessed 06/08/2011).

Certainly, for Second Life to exist as a social community, it must be populated by users who participate actively (cf. Sangwan et al. 2009). Between 2005 and 2007, Second Life was undoubtedly the most popular cybercommunity – it was on the cover of magazines, extensively reported on the well-known *Cable News Network (CNN)* and frequently featured on TV shows and documentaries (Scoble 2010). Despite recent questions as to why Second Life has past its prime,[7] there is strong counter evidence for the continuing popularity and rise of Second Life (e.g. Takahashi 2010). Seven years after its launch to the public, in March 2010, Linden Lab reported that Second Life had more than 1 million active residents[8] and virtual participation of more than 1,400 corporations, universities and government agencies (Vollmer 2010). On August 5, 2011, 21,141,990 user accounts were recorded in Second Life (Childs 2011). Philip Rosedale once told a Second Life blogger that about only 10% of newly created residents are still signing in weekly, three months later.[9] Based on this percentage, on August 5, 2011, there were more than two million active residents in Second Life. Moreover, Second Life continues to be a community with a functioning and successful economy. Large businesses, such as Air France, Cisco Systems, Dell, IBM and Siemens, are still actively operating in Second Life (Cremorne 2011). In 2009, as the real world economy shrivelled, the Second Life' economy continued to flourish – user-to-user transactions reached US$567 million, a 65% jump over 2008 (Rosenwald 2010). In March 2010 – a time when many other cybercommunities were closing (e.g. Vivaty and There.com) – Second Life had a record month as user-to-user transactions reached US$57 million; transactions for the first quarter of 2010 reached US$160 million, a 30% year-over-year jump (Caoili 2010). In December 2010 alone, about 770,000 unique residents made repeat visits to Second Life and these residents converted US$55 million of their Second Life income in 2010, transferring it to their PayPal accounts (Rosenwald 2010). These figures show that the Second Life social world is still very much alive.

Second Life is, however, also a fantasy world that offers its participants a set of capabilities superior to the physical world – it is a world where the boundary between reality and imagination is truly indistinct; where, through 3D avatars and 'stage-managing' these avatars, individuals can truly be whoever and whatever they want to be, and do almost whatever they want to do – possess fantasy physical characteristics, lead idealised lifestyles, fly without wings. The sociability and real world tradability of life in Second Life coupled with its fantasy elements lead to questions such as "If Second Life isn't a game, what is it?" (Kalning 2007). Actually, the question as to whether Second Life should be perceived as an online game is fundamental to research on deviance in the environment and to the intellectual depth of this article.

Thus, it needs to be emphasised that Second Life differs significantly from many offline computer games and online virtual reality games – it is a cybercommunity. For Curtis (1992), "[a cybercommunity] is not goal-oriented; it has no beginning or end, no 'score', and no notion of 'winning' or 'success'… [such an online environment] isn't really a game at all" (ibid: 122). Certainly, Second Life is not a game programmed by game creators and played by game players. Treating such an environment as a game would confuse online sociality with competition and entertainment, therefore, dismissing forms of intimacy, community and political economy in Second Life (Boellstorff 2008). Moreover, Second Life is also very different from popular online social software, such as Facebook and Twitter, which are social networking sites – designed for real world people to maintain real world contact. Thus, Second Life is different; it is a genuine social community, one where people can live out an authentic and 'full' alternative virtual 'physical' existence (Boellstorff 2008).

[7] This is evident in news articles, such as "What happens to Second Life?" (Hanson 2009) and "How to save Second Life in Seven Easy Steps" (Wjamesau 2010), as well as personal blogs, such as "Why I hardly ever go on Second Life anymore" (Wagner 2011).

[8] Individuals who log in Second Life to activate their avatars regularly.

[9] See: http://nwn.blogs.com/nwn/2006/11/new world numbe.html (accessed 10/03/08).

This conception makes Second Life an authentic and fertile ground for criminological research. In contrast to the volume of literature about deviance in the physical world, there is, at this moment, a limited understanding of deviance in cybercommunities, especially from first-hand empirical research (e.g. Williams 2003). Moreover, existing research on deviance in cybercommunities tends to situate the field of enquiry in the wider and more advanced field of cybercrime, and tends to focus on the idea that some fundamental characteristics of the Internet in general, and cybercommunities in particular, are responsible for high levels of deviance or crime (e.g. Williams 2006; Yar 2006; Wall 2007). To distinguish deviance from crime, Williams (2003) suggests that in contrast to cybercrime in which networked computers are used to perpetrate criminal acts, deviance in cybercommunities can be defined as activities that contravene social norms and values – and such cybercommunities are commonly perceived as fertile grounds for deviance to manifest. The environment of cybercommunities may be characterised as an 'unregulated bandit country', where deviance flourishes as a result of "The relative freedom individuals may feel by being untied from material commitments of the offline world" (Williams 2003: 185). Indeed, whether evidence-based or not, the public link between cybercommunities and deviance is strong (Wall 2011). In particular, the 'dark side' of Second Life has attracted much attention from the media, promoting the idea that cybercommunities are deviance-ridden (e.g. Holahan 2006; O'Hear 2006; Black 2007; Lynn 2007; Stanage 2007; Reuters 2008a; Rivington 2008; Warrant and Palmer 2011).

Certainly, Second Life has its darker side – different forms of deviant acts do occur in the cybercommunity. These include general deviant acts in cyberspace, such as cyber harassment, cyber trespass, cyber theft, cyber obscenity and cyber violence; and specific acts that have been identified by Williams' (2003) empirical research in the cybercommunity Activeworlds, such as profanity, flooding[10] and vandalism. However, since Second Life is known for its sociability, instead of using terminologies of a legalistic manner, deviant acts in the cybercommunity are described in Second Life Community Standards[11] in a language that is easily understood by its residents and outsiders. Specific deviant acts include those that have been prohibited by the *Big Six* governing principles of behaviour in Second Life. Next, we deal with each of these in turn.

Intolerance concerns behaviours that belittle or diminish individuals, groups in Second Life, or the Second Life community as a whole, e.g. the use of derogatory language or images against another resident's religion, gender, race, ethnicity or sexual orientation. *Harassment* includes activities that are carried out in a manner which is offensively coarse, intimidating or threatening, e.g. unwelcome sexual advances. *Assault* pertains to shooting, pushing, or shoving another resident in areas where these acts are strictly prohibited by Second Life, as well as creating or using scripted objects to target another resident in a manner that would prevent the targeted resident from enjoying their Second Life experience. *Disclosure* mainly deals with the revelation of another resident's real world personal details that are not volunteered in his resident profile, including gender, religion, age, marital status, race, sexual preference and alternate account names. Disclosure also refers to the violation of another residents' privacy in Second Life, which includes remotely monitoring conversations, posting conversation logs, or sharing conversation logs without consent. *Adult regions, groups, and listings* concerns 'adult' content, activity and communication, especially those of a sexual nature. Although Second Life is an adult community, it is separated into different regions, such as 'adult', 'moderate' and 'general' – any 'adult' content that falls under Second Life's Adult Maturity Definition[12] is only allowed in 'adult' regions. *Disturbing the peace* refers to the disruption of scheduled events, the repeated transmission of unwanted advertising material, the use of

[10] Flooding is exemplified by the act of uploading excess amount of advertising materials to slow down server performance.

[11] See: http://secondlife.com/corporate/cs.php (accessed 08/08/2011).

[12] See: http://community.secondlife.com/t5/English-Knowledge-Base/Maturity-ratings/ta-p/700119#Adult (accessed 06/08/2011).

repetitive sounds, etc. It is also concerned with any activities that would reduce server performance or hinder other residents' ability to enjoy life in Second Life.

High profile cases of deviance in Second Life include the 'Wonderland Sandal', the 'Abduction Sandal', the 'Virtual Rape Scandal'[13] and the 'CopyBot Scandal'. Wonderland is a place in Second Life where child-like avatars were found to be offering virtual sex to other avatars (Nino 2008). In August 2008, a woman was charged in the US State of Delaware with plotting the real-life abduction of a boyfriend she met in Second Life.[14] In April 2007, two Belgian newspapers reported that the Brussels public prosecutor had asked the Federal Computer Crime Unit to enter Second Life to investigate a virtual rape involving a Belgian citizen (Duranske 2007). CopyBot is a program that enables the copying of another user's content without permission (Holahan 2006) – a violation of both the Digital Millennium Copyright Act (US DMCA) and the Second Life Term of Service.[15]

Social and Technological Development of Surveillance

The rise of surveillance is attributed to the growing need for security – "the condition of 'being protected from threats' " (Zedner 2009: 14). The growing need for security and the growing perception of this need, reflect the wider insecurity of the modern world. In the modern world, crime is considered as a "normal social commonplace aspect of modern society" (Garland 2001: 128). Given this, it has been argued that crime needs to be reconceptualised as "risk to security" and "demands intervention before crimes occur, on the grounds that where the risks can be calculated it is more cost effective to prevent loss than to punish retrospectively" (Zedner 2009: 71).

The focus on crime intervention and prevention leads to the emphasis on control of behaviours of large groups and individuals. This emphasis both necessitates and leads naturally and in a common sense manner to the use of advanced technologies to collect and process data. Thus, various technologies are adopted to manage risk. Actions and events are addressed by Closed-Circuit Television (CCTV) camera surveillance, Automatic Number Plate Recognition (ANPR) systems and electronic monitoring of convicted offenders. Personal identities are managed with Radio Frequency Identification (RFID) cards, PIN numbers, biometric recognition systems, iris scans and DNA profiling. These forms of surveillance technologies enable the recording, storing and processing of surveillance data in digital forms across time and space, thus turning the concept of 'global surveillance' into a realistic prospect (cf. Coleman and McCahill 2010).

In turn, the adoption of these surveillance technologies further stimulates the rise of surveillance. For Coleman and McCahill (2010), "surveillance has a tendency to disperse and become operative in a wide range of social settings ... and by its complexity, sprawl and spatial decentralisation it tends to become self-sustaining so that surveillance and control leads to more surveillance and control" (ibid: 19). During the past two decades, there has been a significant and continuous growth in the use of surveillance technologies both in number and applications. The number of CCTV cameras has grown significantly in the UK, US and other Western nations (Welsh and Farrington 2008). For example, in the UK, the number of surveillance cameras increased from 100 in 1990 to 400 in 1994, to 5,200 in 1997, to 40,000 in 2002 (Armitage 2002). In 2006, there were up to 4.2 million CCTV cameras in Britain – about one for every 14 people, which means that the UK had 1% of the world's population but 20% of its CCTV cameras (BBC News 2006). Moreover, CCTV cameras are integrated into different forms of surveillance technologies, such ANPR. Recently, there are 10,502 ANPR cameras collecting data for police forces (Mathieson

[13] Virtual rape can be understood as forced online sexual activity through text, animation, malicious script, etc. (Dibbell 1993).

[14] See: http://www.independent.co.uk/life-style/gadgets-and-tech/news/woman-jailed-after-killing-virtual-husband-972457.html (accessed 06/08/2011).

[15] See: http://secondlife.com/corporate/tos.php (accessed 06/08/2011).

2010). In terms of electronic monitoring of convicted offenders, the Global Positioning System (GPS) has been increasingly adopted to track offenders in the US since 1997 and has been piloted in a number of European countries, including Germany, England, Wales, France and the Netherlands (Nellis 2008). By 2000, England and Wales had the most thorough electronic monitoring scheme in Europe (ibid 2008). In data profiling, the emergence of 'blanket DNA testing' of an entire community – where everyone in a specific community is treated as a 'suspect' until the 'risk profile' proves otherwise (McCahill and Norris 2003) – is an example of the potential of surveillance technology to target entire human populations.

Moreover, the heavy monitoring of everyday life includes surveilling activities on the Internet. The wiretapping of telephones has been extended through email to Internet clickstream monitoring (Lyon 2003). In 2009, the UK government planned to give police and security services the power to snoop on every single communication made by the public with the data then likely to be stored in an enormous national database (Whitehead 2009). In October 2010, the UK government's "*Security Britain in an Age of Uncertainty: The Strategic Defence and Security Review*" introduced the Interception Modernisation Programme (IMP), which would monitor all residents' email accesses and website visits (not the actual contents of the websites) and store these data for a period of one year (HM Government 2010). Actually, due to the technological structure of the Internet, surveillance technologies have the potential to be carried out far more forcefully and to work far more vigorously online than offline. In the world of the Internet, it is possible to replace rules and norms with codes (Lessig 1999) – inscribe social rules and norms into algorithmic formulae – and to render deviance impossible because "the norm becomes a technical rule of action" – a kind of "neutral parameter independent of decisions and values" (Lianos and Douglas 2000: 108). The world of the Internet can be created as an environment, where "discretion and moral judgement are peripheral in the sense that the former is almost non-existent and the latter has become a technical issue" (Coleman and McCahill 2010: 23). For example, in 2009, the Chinese Government decided to install the *Green Dam Youth Escort* web filter on all PCs sold in China, in order to protect children from Internet contents, such as pornographic, violent and other "unhealthy" websites (Chen and Wang 2009). Actually, in theory, it is perfectly possible to turn the world of the Internet into a digital panopticon, where all people from all walks of life are now monitored (cf. Haggerty and Ericson 2006).

Indeed, with the aid of technologies, the surveillance gaze has been expanded to a level unimaginable in the physical world. This expansion leads to a power imbalance between the surveilled and the surveillance regime – there is hardly any room for the surveilled to negotiate with the surveillance regime. On the one hand, the information captured by surveillance technologies, such as CCTV cameras, is systematically stored on a computer file or videotape, ready to be lifted out at some future, as yet unspecified time and place (McCahill 2002). On the other hand, to the surveilled, there is no way of knowing "how, where and when data about us is stored, how our identities are fabricated within the 'data image' (Lyon 1994) or the 'data-double' (Haggerty & Ericson 2000)" (Coleman and McCahill 2010: 20).

Surveillance Capability and Practice in Second Life

Existing in the world of the Internet, the cybercommunity Second Life has a complete governance structure. Since Second Life is owned by Linden Lab, the Lab has a total control over the cybercommunity. All residents in Second Life agree to observe the Community Standards and the Terms of Service, especially the *Big Six*. Transgressors of the *Big Six* can be warned, suspended or even permanently banished from Second Life by Linden Lab, by sending warning emails, suspending user accounts or cancelling user accounts. Of course, an individual is able to keep his actual life identity secret from other residents in Second Life, since anyone can register for an account anonymously. However, on principle, Linden Lab's registration policy requires accurate personal information to prevent individuals from safeguarding their real-life identities – a resident's Second Life account name is the same as his avatar in Second Life. Thus, Second Life residents' personal information is directly associated with their avatar identity. Linden Lab, therefore, have the power to connect online and offline identities in ways that its residents are unaware (Lo 2008). Thus, although it happens rarely, real world sanctions are not out of reach for Linden Lab upon contacting real world justice processes (Boellstorff 2008).

Once an individual enters Second Life after registration, there is absolutely no privacy for his avatar in Second Life – Linden Lab is watching and recording all the time – and the potential for in-world Second Life sanctions is ever present. Every single item in Second Life, such as a typed word, a simple gesture, a conversation via Voice over IP (VoIP) or, indeed, every single action is recorded and stored in the database of Isilon Systems, Inc.[16] On December 13, 2007, the creator of the Second Life software, Philip Rosedale said: "People in Second Life have created over 1 billion in-world 'objects' occupying total storage space of about 100 terabytes".[17] All these 'objects' are perfectly archived and can be pored over at any time.

Moreover, there is an abundance of new technologies available in Second Life that can be used for surveillance purposes. In fact, technological systems that monitor avatar activity and identify risky behaviour are built into the architecture of the Second Life software (Lo 2008). For example, all financial transactions in Second Life are monitored and reviewed electronically, and Linden Lab staff review some of these transactions (ibid). Thus, Linden Lab is able to expand its active monitoring of financial transactions to the active monitoring of all activities in Second Life. For another example, Linden Lab subjects its residents to targeted advertising by monitoring their conduct in nearby areas. In 2007, the Lab allowed AMPP Media – an advertising company – to place digital billboards within Second Life (Burns 2007). Unlike normal billboards, these ones are able to scan for keywords in public conversations in nearby areas and serve advertisements contextually.[18] Technologically, these billboards are perfect tools for data mining, which seeks rules for the classification of objects (cf. Gandy 2007). Data mining can be used to access and rank high or low risk individuals and groups in relation to deviant activities, as well as be used in the prediction of future behaviour and pre-empt deviant behaviours in Second Life.

With the availability and power of such advanced surveillance technologies, theoretically, Linden Lab could detect all violations of the *Big Six* and respond to violators according to the established systems of sanctions using technological systems, e.g. digital billboards. But, in practice, the Lab chooses not to exercise its technological power of detection and punishment. Instead, residents are encouraged to report violations of the Community Standards using the *Abuse Reporter* application, which is located under the *Help* menu in the tool bar. Between June 2007 and September 2009, there were 21,665 recorded and published incidents.[19] During that time frame, between two and three million individuals participated in Second Life, which means between about 0.7% and 2% of the total user base for that period was recorded to have violated the Community Standards.[20] These figures suggest that Second Life is a much safer

[16] Isilon Systems is a global company physically headquartered in Seattle, USA. It designs and sells storage systems and software for digital content and other unstructured data, including Instant Messages (IMs), avatar shapes and appearances, Linden Scripting Language (LSL) scripts, digitised audio clips, the design of every building, etc. On February 26, 2007, Isilon Systems announced: "10 new additions to its growing community of customers who are driving innovation in the emerging world of Web 2.0 content and services. Linden Lab (creator of the Second Life 3D virtual world), Current TV, Dailymotion, FlipClip, Imeem, Jump TV, Pandora TV, PhotoBox, Revver and Skyrock are the latest companies to select Isilon IQ clustered storage as the core technology for access and storage of the ever-expanding user-created digital content assets that are a hallmark of the next generation of Internet interactivity" (see: http://www.isilon.com; accessed 02/08/2010).

[17] See: http://freakonomics.blogs.nytimes.com/2007/12/13/philip-rosedale-answers-your-second-life-questions; accessed 04/08/2011. The total storage space of 100 terabytes is equal to the total Internet traffic in 1993 (100 terabytes = 104857600 megabytes) (http://www.disco-tech.org/2007/10/an\exabyte\here\an\exabyte\the.php; accessed 04/08/2011).

[18] To provide advertisements to individual residents based on a collated 'interest profile', which includes a resident' name and age, where the resident spends time in Second Life, the style of clothing the resident currently wears, etc. (see: http://adverlab.blogspot.com/2007/04/contextual-advertising-in-second-life.html; accessed 04/08/ 2010).

[19] See: http://nwn.blogs.com/nwn/2009/09/crime-scene.html (accessed 05/07/2010).

[20] See: http://nwn.blogs.com/nwn/2009/09/crime-scene.html (accessed 04/08/2010).

environment than most areas in the real world. For example, in the UK, the area with the lowest reported crime rate – Dyfed-Powys, a large rural police region of Wales recorded 48 crimes per 1,000 residents between 2008 and 2009 (4.8%) (Walker et al. 2009).

Of course, there are many sub-communities in Second Life. Some of these sub-communities own a huge amount of land and set their local rules. For example, the management group of Azure Island asks all residents and guests not to harass others, have over aggressive security systems and create computer scripts or virtual objects that impact on the servers negatively.[21] The management group of Azure Island separates its islands into three different zones: residential, commercial and protected. Each of these zones has a unique set of rules and building regulations. Residents in Azure Island are asked to respect these rules and building regulations. Moreover, a resident in Second Life is able to create his own group. The group creator has the right to grant or refuse membership. Nevertheless, owners of these sub-communities and groups can only ask residents to obey their rules and regulations, and identify unwanted behaviours and rule breakers. They do not have the technological power that Linden Lab has to punish. However, the owners have the power to banish wrongdoers from their communities and groups. They are also able to record everything that goes on in their communities and groups, and review the recorded data at any time. In fact, Second Life's Terms of Service[22] do not prohibit investigative inquiry as long as 'remote conversation monitoring' and 'conversation logs' are not used while carrying out an inquiry. Thus, any resident is able to monitor activity in Second Life. Furthermore, according to Boellstorff (2008), for certain serious offences, such as attempting to crash the Second Life software or to gain real world life information about another avatar, e.g. credit card numbers, Linden Lab staff would seek support from real world justice processes. For example, in 2008, Philip Rosedale asked the Federal Bureau of Investigation (FBI) to investigate denial of service attacks in Second Life (Reuters 2008b). Nevertheless, if the accused lives outside the United States, law enforcement could be very difficult (Wall 2001).

Besides these limited options, Linden Lab is the only governing body in Second Life that is able to deal with offences by carrying out formal methods of punishment, including warning, suspension and cancellation of account – none of these extend beyond Second Life to reach the person physically. Moreover, in order not to appear dictatorial – and thus, to act against Second Life's original design and ideology of "a public park with minimum rules" (Guest 2007: 73) – Linden Lab staff hesitate to act against residents unless a clear violation of the Terms of Service is documented (Malaby 2006). Hence, instead of creating a virtual dictatorship, Linden Lab's user-content model of community building has driven its governmentality towards the implicit (ibid) – as such much of Linden Lab's governance operates at the level of setting norms, rather than managing daily interactions (Boellstorff 2008).

Personal and Social Bond in Second Life

Based on the central question – Why do individuals obey the rules of society? – social bonding theory[23] assumes that deviant acts occur when an individual's bond to society is subject to atrophy (Hirschi 1969). Based on data collected, we suggest that it is because of the importance and value of these personal and social bonds that individuals within Second Life choose to obey global and local rules and norms in the cybercommunity, and that the power of these social bonds functions to regulate the behaviour of Second Life residents in its diverse communities.

This suggestion is in sharp contrast to current understanding of cybercommunities wherein individuals feel free to indulge in activities that contravene common social norms and values (Williams 2003). This view

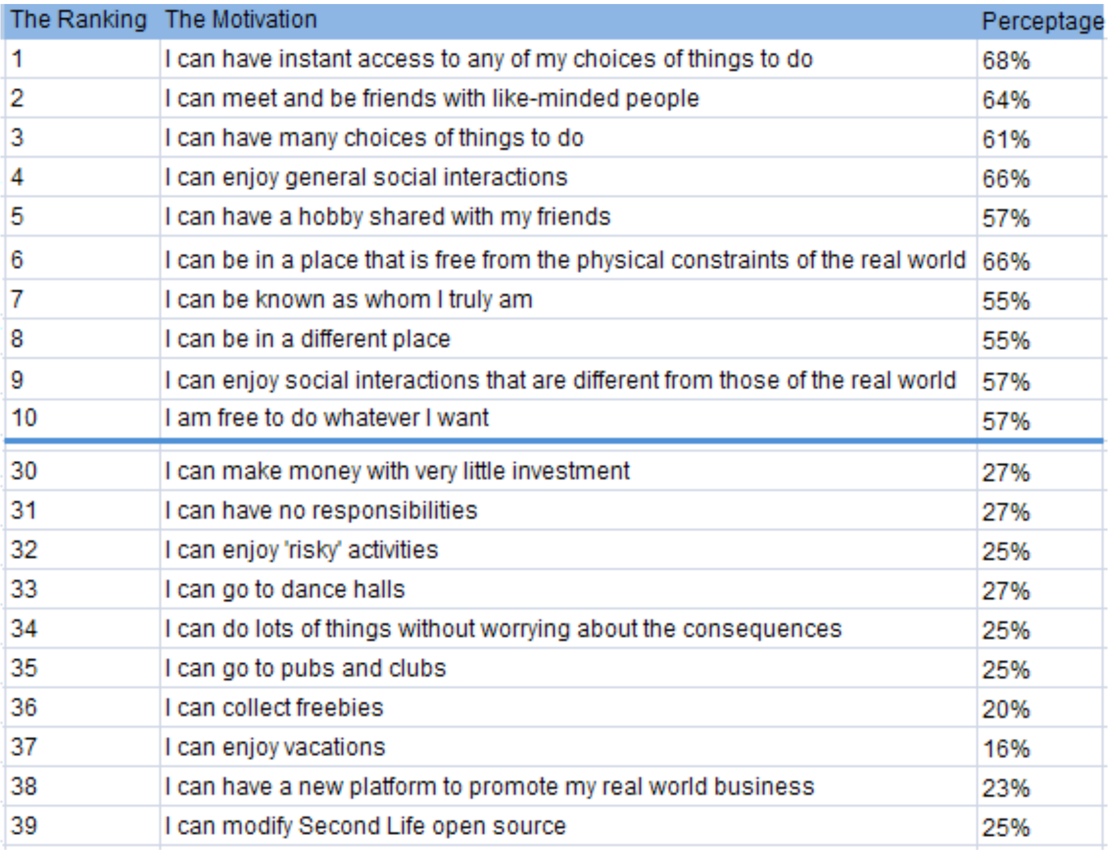
[21] See: http://azure.anshex.com (accessed 04/08/2010).

[22] See: http://secondlife.com/corporate/tos.php (accessed 04/08/2011).

[23] Hirschi's (1969) control theory is referred as social bonding theory in this article to distinguish it from early control theories and self-control theory.

is attributed to a weak sense of community in the environments (ibid) which is, in turn, associated with the freedom to act without restraint due to the proffered anonymity of cybercommunities (e.g. Demetious and Silke 2003). Our data demonstrates that the category of community related motivations is the second most motivating property behind individuals' participation in Second Life: more than 65% of the participants are 'very much' or 'quite a lot' motivated by being able to enjoy general social interactions; more than 60% of the participants are 'very much' or 'quite a lot' motivated by being able to meet and be friends with like-minded people and more than 47% of the participants are 'very much' or 'quite a lot' motivated by being able to belong to a community.

Social bonding theory assumes that if individuals invest time and energy to carry out various forms of conventional activities in a society, they would not want to risk losing their investment by engaging in activities that breach the rules of that society. Moreover, involved heavily in these conventional activities, individuals may be too busy to consider performing deviant activities. Following these, conventional activities in Second Life would bring individuals together and form the fabric of social control in the cybercommunity. What are conventional activities in Second Life? We suggest that since, in most cases, participation in Second Life is purely optional, conventional activities in the cybercommunity should be the reasons that most motivate participation in Second Life. In our research (Wang 2009), nine out of the top ten motivations[24] are related to pursuing a multitude of choices, finding friends, enjoying social interactions and pursuing a sense of self; whereas some of the bottom ten motivations may be associated with different degrees of triviality and playfulness (see: Table 1).



The Ranking	The Motivation	Perceptage
1	I can have instant access to any of my choices of things to do	68%
2	I can meet and be friends with like-minded people	64%
3	I can have many choices of things to do	61%
4	I can enjoy general social interactions	66%
5	I can have a hobby shared with my friends	57%
6	I can be in a place that is free from the physical constraints of the real world	66%
7	I can be known as whom I truly am	55%
8	I can be in a different place	55%
9	I can enjoy social interactions that are different from those of the real world	57%
10	I am free to do whatever I want	57%
30	I can make money with very little investment	27%
31	I can have no responsibilities	27%
32	I can enjoy 'risky' activities	25%
33	I can go to dance halls	27%
34	I can do lots of things without worrying about the consequences	25%
35	I can go to pubs and clubs	25%
36	I can collect freebies	20%
37	I can enjoy vacations	16%
38	I can have a new platform to promote my real world business	23%
39	I can modify Second Life open source	25%

[24] Except the 10th "I am free to do whatever I want".

Table 1: The top and bottom 10 motivations on the list of the 39 motivations (1 being the most motivating). The motivations are ranked based on their mean scores. The percentage in the table is the percentage of participants who are 'very much' or 'quite a lot' motivated by the property.

Perhaps, it can be argued that one of the top ten motivations: "I am free to do whatever I want" is associated with degrees of playfulness and carelessness, which are often linked to deviance (Williams 2003). Nevertheless, both "I can have no responsibilities" and "I can do lots of things without worrying about the consequences" are among the reasons that least motivate participation in Second Life. This may suggest that individuals do not consider Second Life as a place where they can be free from responsibilities and they are aware of the consequences of their actions in Second Life. The data leads to the possibility that the participants who are 'very much' (25%) and 'quite a lot' (32%) motivated by "I am free to do whatever I want" are merely pursuing a set of activities that can be carried out in Second Life, but cannot be carried out in the real world. For example, among the numerous possibilities in Second Life – expanding far beyond real world possibilities – that our correspondents reported as motivations for participating in Second Life, the ability to express an alternative physical identity is a significant one (e.g. Furry[25]).

Nevertheless, Second Life consists of thousands of sub-communities and groups; some are designed to carry out activities that may be considered as deviant in the cybercommunity as a whole. However, to participants in these sub-communities and groups, these activities are naturally considered to be conventional. This was clearly articulated by one of our correspondents in an open forum discussion:

> Various communities often specify rules of behaviour for the activities they support. These are more detailed for specific people involved. Other communities do the same for people visiting ... a social group will ban public nudity or certain activities in their areas, for example. One adapts to the norms of the community, or leaves it if one cannot (Forum correspondence, March 5, 2009).

In this case, a strong sense of attachment to the sub-communities and groups and individuals in these may lead to more individuals engaging in deviant behaviour and more opportunities for the extent of deviance to both broaden and deepen, if the norms of these sub-communities and groups are deviant in the Second Life community as a whole. However, our data shows that most individuals do not participate in Second Life to join some deviant groups. The extract below demonstrates how strongly individuals in Second Life feel about the general assumption that everyone in Second Life is here to carry out activities that deviate from social rules and norms of the real world:

> Anyone who actually knows this topic will tell you that "deviant" behaviour is actually just behaviour that people don't discuss in public. "Normal" people engage in all sorts of things that might be considered "deviant" – as many previous studies have shown. It's only "deviant" if it's something you yourself don't do.
> P**** answer: I'm really f***ing tired of the assumption that everyone in SL is there for fetish sex (Forum correspondence, March 4, 2009).

More importantly, activities in sub-communities and groups are closely monitored by their owners and restricted to their membership. Although, as mentioned previously, these owners do not have the technological power to punish rule breakers – rule breakers can be banished by the owners and ostracised

[25] A Furry is a fox-like anthropomorphic animal character. By Rymaszewski et al. (2007), the Furry is the most well represented group of residents in Second Life.

by the rest of the group as outsiders since these communities are built on, and maintained by, close personal bonds among their members.

Actually, even Linden Lab's three forms of punishment – warning, suspension and cancellation of account – depend on social and personal bonds. If a resident spends a significant amount of time and energy in creating his avatar and building relationships with other residents then he has much to lose if his account is cancelled. On the other hand, if the resident considers his participation in Second Life as trivial, then he may not be too concerned about cancellation. Moreover, Second Life uses an email-address based registration system – this resident can simply join Second Life again using a different email account. Of course, the resident's computer Internet Protocol (IP) address could be traced and his computer blocked, but this can be easily subverted by using a different computer. It is generally well known that IP addresses are randomly generated by Internet Service Providers (ISP) and change periodically. Contacting the ISP of the resident and asking the ISP to cease providing Internet service may be subverted by switching to a different service provider.

In short, the infrequent manifestation of deviance in Second Life is intimately associated with an individual's bond with the cybercommunity and with other individuals in the cybercommunity as a whole, sub-communities or groups. It is precisely because of this bond that individuals in Second Life choose to conform to the norms and rules.

Conclusion

In the real world, the rapid growth in surveillance technologies seems to be sending two messages – firstly, surveillance technologies are good for society and, secondly, the shortcomings of surveillance technologies can be resolved by more or better surveillance technologies in policing and related functions.

Pursuing this belief and its consequences, we have considered extreme cases of communities where surveillance approaches "perfection". In particular, we have analysed the cybercommunity Second Life – a social realm that is totally represented and captured by technology, where code can be law (Lessig 1999). Second Life is a place where there is an abundance of surveillance technologies that can be used to collect and store a vast amount of information and where moral judgment can be reduced to a technical issue and even automated. In such a place, it is natural to assume that surveillance technologies are heavily used to control and regulate deviance and are effective in controlling and regulating deviance.

However, we have argued that although Second Life is totally constructed by technology, the software technologies are not prominent and are, in fact, downplayed as mechanisms or processes to deal with deviance. It is clear that the authority (Linden Lab) responsible for Second Life does not want to use technologies of surveillance, report and punishment that are not sociologically native to Second Life to govern the cybercommunity. After all, the creator of the Second Life software, Philip Rosedale, intended to design a virtual world comparable with and transcendent of the real world, as well as a place with minimum rules (Guest 2007). For Rosedale, in the long term, Second Life would have to develop its own standards of behaviour and the thousands of sub-communities and groups would develop their local authorities to deal with various forms of deviance (Holahan 2006). Our evidence suggests that this has happened. We have shown that in Second Life, instead of surveillance technologies, it is the power of relationship that brings individuals together to conform to the rules and norms – forming the fabric of social control and the regulation of deviance. Even the effectiveness of Linden Lab's three technological forms of punishment depends on social and personal bonds.

Our findings are in line with the more general discovery that as behaviour on the Internet is becoming increasingly socially complex, techno-centered and techno-mediated methods of policing are gradually moving away from being the main and most effective category of method in controlling and regulating criminal/deviant behaviour online (Wall and Williams 2007; Williams 2007). In their place, methods in the category of societal policing (Gill 1994) are becoming more prominent. In the more specific environment of cybercommunities, as these communities become more connected to their participants' physical and emotional life, proximal (online) nodes of governance, such as reputation management systems, vigilante groups that employ 'online shaming' and virtual 'police' services, are developing rapidly and are proving to be effective (Williams 2007).

In short, our research has shown that cybercommunities have a rich sociology that can help to examine ideas and assumptions about individuals and social groups, communities and societies. From the viewpoint of our research on cybercommunities, a major motif in policing in the real world – surveillance through technologies – becomes questionable, both in the nature of the social ideas and assumptions underpinning it and in the scope of its applications and effects.

References

Armitage, R. 2002. To CCTV or Not to CCTV? A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime. *Community Safety Practice Briefing*, Nacro.

BBC News. 2006. Britain is 'surveillance society'. *BBC News*, 2 November. Available at: www.news.bbc.co.uk/1/hi/uk/6108496.stm.

Black, S. 2007. Cyber crime set to explode in Second Life? *crikey.com*, 14 May. Available at: www.crikey.com.au/2007/05/14/cyber-crime-set-to-explode-in-second-life.

Boellstorff, T. 2008. *Coming of Age in Second Life*. Princeton University Press.

Burns, E. 2007. New Ad Network Integrates Digital and Outdoor Media. *ClickZ*, 16 April. Available at: www.clickz.com/clickz/news/1707176/new-ad-network-integrates-digital-outdoor-media.

Caoli, E. 2010. Second Life's User Transactions Hits Record $57M in March. *GAMASUTRA*, 29 April. Available at: www.gamasutra.com/view/news/28314/Second_Lifes_User_Transactions_Hits_Record_57M_In_March.php.

Carr, P. and Pond, G. 2007. *The Unofficial Tourists' Guide to Second Life*. Boxtree.

Chen, T.M. and Wang, V. 2010. Web Filtering and Censoring. *Computer, IEEE Computer Society* March 2010: 94-97.

Childs, A. 2011. Adz Childs' Personal Blog. *SLNameWatch.com*, 5 August. Available at: slnamewatch.com.

Coleman, R. and McCahill, M. 2010. *Surveillance & Crime*. Sage: Los Angeles, London, New Delhi, Singapore, Washington DC.

Cremorne, L. 2011. Large businesses in Second Life: they still exist. *The Metaverse Journal*, 27 March. Available at: www.metaversejournal.com/2011/03/27/large-businesses-in-second-life-they-still-exist/.

Curtis, P. 1992. Mudding: Social Phenomena in Text-based Virtual Realities. In: Kiesler S (ed) *Culture of the Internet*. Mahwah, NJ: Lawrence Erlbaum Associates.

Demetious, C and Silke, A. 2003. A Criminological Internet "Sting": Experimental Evidence of Illegal and Deviant Visits to a Website Trap", *British Journal of Criminology* 43(1): 213-222.

Dibbell, J. 1993. A Rape in Cyberspace, or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society. *The Village Voice* December 23: 36-42.

Duranske, B. 2007. Reader Roundtable: "Virtual Rape" Claim Brings Belgian Police to Second Life. *Virtually Blind*, 24 April. Available at: virtuallyblind.com/2007/04/24/open-roundtable-allegations-of-virtual-rape-bring-belgian-police-to-second-life/.

Farrington, D.P., Bennett, T.H. and Welsh, B.C. 2007. The Cambridge Evaluation of the Effects of CCTV on Crime. In: Farrell, G. (ed) *Imagination for Crime Prevention: Essays in Honour of Ken Pease* Monsey, N.Y.: Criminal Justice Press.

Finn, R. and McCahill, M. 2010. *Representing the Surveilled: Media Representation and Political Discourse in Three UK Newspapers*. Copyright PSA 2010. Available at: www.psa.ac.uk/journals/pdf/5/2010/266_348.pdf.

Gandy, O.H. 2007. Data mining and surveillance in the post-9/11 environment. In: Hier SP and Greenberg J (eds) *The Surveillance Studies Reader*. Berkshire: Open University Press.

Garland, D. 2001. *The culture of control: Crime and social order in contemporary society*. Oxford: Oxford University Press.

Gill, M. 1994. *Crime at Work: Studies in Security and Crime Prevention*. Leicester: Perpetuity Press.

Gill, M. and Spriggs, A. 2005. Home Office Research Study 292: Assessing the Impact of CCTV. Home Office Research, Development and Statistics Directorate. Available at: www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf.

Gill, M., Spriggs, A., Little, R. and Collins, K. 2006. What do murderers think about the effectiveness of CCTV?, *Journal of Security Education* 2(1): 11-17.

Goodwin, V. 2002. *Evaluation of the Devonport CCTV Scheme*. Hobart, AUS: Crime Prevention and Community Safety Council, Tasmania Police.

Griffiths, M. 2003. *Town centre CCTV: An examination of crime reduction in Gillingham, Kent*. Reading, UK: University of Reading. Available at: www.crimereduction.homeoffice.gov.uk/cctv/cctv33.pdf.

Guest, T. 2007. *Second Lives* Hutchinson London.

Haggerty, K.D. and Ericson, R.V. 2000. The surveillant assemblage. *British journal of Sociology* 51(4): 605-622.

Haggerty, K.D. and Ericson, R.V. 2006. The new politics of surveillance and visibility. In: Haggerty KD and Ericson RV (eds) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Hansen, L. 2009. What happened to Second Life. *BBC News Magazine*, 20 November. Available at: news.bbc.co.uk/1/hi/8367957.stm.

Hirschi, T. 1969. *Causes of Delinquency* Berkeley, Los Angeles, and London: University of California Press.

HM Government. 2010. *Security Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. HM Government 2010. Available at: www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr.

Holahan, C. 2006. The Dark Side of Second Life *Businessweek*, 21 November. Available at: www.businessweek.com/technology/content/nov2006/tc20061121_727243.htm.

Kalning, K. 2007. Is Second Life isn't a game, what is it? – Many have struggled with how to characterise 3-D online virtual world. *msnbc.com*, 3 December. Available at: www.msnbc.msn.com/id/17538999/ns/technology_and_science-games/t/if-second-life-isnt-game-what-it/.

Jones, R. 2005. Surveillance. In Hale C, Hayward K, Wahidin A and Wincup E. (eds) *Criminology*. Oxford: Oxford University Press.

Lessig, L. 1999. *Code and other laws of cyberspace* Basic Books: New York.

Lianos, M. and Douglas, M. 2000. Dangerization and the end of deviance: the institutional environment. In: Garland D and Sparks R (eds) *Criminology and Social Theory*. Oxford: Oxford University press.

Lindberg, O. 2007. Interview *Philip Rosedale.net*, 8 February. Available at: www.netmag.co.uk/zine/discover-interview/philip-rosedale.

Locke, L. 2007. The Future of Facebook. *Time Magazine*, 17 July. Available at: www.time.com/time/business/article/0,8599,1644040,00.html.

Lo, J. 2008. Second Life: Privacy in Virtual Worlds. Office of the Privacy Commissioner of Canada. Available at: www.priv.gc.ca/information/pub/sl_080411_e.cfm#sec45.

Lynn, R. 2007. Virtual Rape Is Traumatic, but Is It a Crime? *Wired.com*, 5 April. Available at: www.wired.com/culture/lifestyle/commentary/sexdrive/2007/05/sexdrive_0504.

Lyon, D. 1994. *The Electronic Eye: The Rise of the Surveillance Society*. Cambridge: Polity Press.

Lyon, D. 2003. Surveillance Technology and Surveillance Society. In: Misa TJ, Philip B. and Feenberg A (eds) *Modernity and Technology*. Cambridge Mass.: MIT Press.

Lyon, D. 2007. *Surveillance studies: An overview*. Cambridge: Polity Press.

Malaby, T.M. 2006. Coding Control: Governance and Contingency in the Production of Online Worlds, First Monday, special issue 7, invited presentation for The Speaker Series, American Bar Foundation, Chicago, Illinois.

Mathieson, S.R. 2010. The ANPR secret – Police forces are making extensive use of their numberplate cameras, but proving coy about their locations. *Guardian Government Computing*, 3 February. Available at: www.guardian.co.uk/government-computing-network/2010/feb/03/automatic-numberplate-recognition-police-anpr-gc-feb10.

McCahill, M. 2002. *The Surveillance Web: The Rise of Visual Surveillance in an English City*. Cullompton: Willan.

McCahill, M. and Norris, C. 2003. Victims of surveillance. In: Davis P, Jupp V and Francis P (eds) *Victimisation: Theory, Research and Policy*. Basingstoke: Palgrave Macmillan.

Nellis, M. 2008. Mobility, locatability and the satellite tracking of offenders. In: Aas K, Gundhus H and Lomell H (eds) *Technologies of Insecurity: The Surveillance of Everyday Life*. London: Routledge.

Norris, C. 2003. From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In: Lyon D (ed) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. New York: Routledge.

Norris, C. and Armstrong, G. 1999. *The Maximum Surveillance Society*. Oxford: Berg.

O'Hear. 2006. Second Life: gangs, theft and goo. *ZDnet*, 22 November. Available at: www.zdnet.com/blog/social/second-life-gangs-theft-and-goo/27.

Orwell, G. 1948. *1984 Nineteen Eighty-Four*. Penguin Classics; New Ed edition (2004).

Presdee, M. 2000. *Cultural Criminology and the Carnival of Crime*. Routledge: London and New York.

Reuters, E. 2008a. Virtual retailers decry Second Life crime wave. *Second Life News Center*, 7 February. Available at: secondlife.reuters.com/stories/2008/02/07/virtual-retailers-decry-second-life-crime-wave.

Reuters, E. 2008b. Rosedale discloses FBI griefing probe to Congress. Second Life News Center, 1 April. Available at: secondlife.reuters.com/stories/2008/04/01/rosedale-discloses-fbi-griefing-probe-to-congress.

Rivington, J. 2008. Second Life probed by crime wave cops *techradar.com*, 25 March. Available at: www.techradar.com/news/internet/second-life-probed-by-crime-wave-cops-270599.

Rosenwald, M.S. 2010. Second Life's virtual money can become real-life cash *The Washington Post*, 8 March. Available at: www.washingtonpost.com/wp-dyn/content/article/2010/03/07/AR2010030703524.html.

Rymaszewski, M., Au, W.J., Ondrejka, C. and Platel, R. 2007. *Second Life: The Official Guide*. John Wiley & Sons, Inc., Hoboken, New Jersey.

Sangwan, S., Guan, C. and Siguaw, J.A. 2009. Virtual Social Networks: Towards A Research Agenda *International Journal of Virtual Communities and Social Networking* 1(1): 1 –13.

Scoble, R. 2010. Is Second Life about to enter its "Second Life". *Scobleizer*, 22 February. Available at: scobleizer.com/2010/02/22/is-second-life-about-to-enter-its-second-life.

Stanag,e N. 2007. From Second Life to second-degree murder *Guardian.co.uk*, 1 January. Available at: www.guardian.co.uk/commentisfree/2007/jan/16/fromsecondlifetoseconddegr.

Stephenson, N. 1992. *Snow Crash*. New York: Bantam Books.

Takahashi, D. 2010. Virtual worlds recede, but Second Life keeps growing *GamesBeat*, 28 April. Available at: venturebeat.com/2010/04/28/virtual-worlds-recede-but-second-life-keeps-growing/.

van der Ploeg, I. 2003. Biometrics and the body as information: narrative issues of the socio-technical coding of the body. In Lyon D (ed) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge.

Vollmer, S. 2010. How much life is there in Second Life?. *Science in the Triangle*, 4 April. Available at: scienceinthetriangle.org/2010/04/how-much-life-is-there-in-second-life/.

Wagner, M. 2011. Why I hardly ever go on Second Life anymore. *Copper Robot: Mitch Wagner's old blog*, 14 February. Available at: copperrobot.com/2011/02/why-i-hardly-ever-go-on-second-life-anymore/.

Wall, D.S. 2011. Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society* (11): 861-884.

Wall, D.S. 2007. *Cybercrime*. Cambridge: Polity Press.

Wall, D.S. 2001. Crime and the Internet. London: Routledge, Talor & Francis.

Wall, D.S and Williams, M. 2007. Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology & Criminal Justice* 7(4): 391-415.

Walker, A., Flatley, J., Kershaw, C. and Moon, D. 2009. Crime in England and Wales 2008/2009 – Volume 1 Findings from the British Crime Survey and Police Recorded Crime. Home Office. Available at: news.bbc.co.uk/1/shared/bsp/hi/pdfs/16_07_09_bcs.pdf.

Wang, V. 2009. *Deviance in a Cybercommunity*. Unpublished doctoral thesis, Swansea University, Swansea.

Warrant, T. and Palmer, T. 2011. Crime risks of three-dimensional virtual environments. *slexandcity.com*, 4 April. Available at: www.slexandthecity.com/featured/crime-risks-threedimensional-virtual-environments.

Welsh, C. and Farrington, D. 2008. The Politics of the Selective Gaze: Closed Circuit Television and the Policing of Public Space. *Crime, Law and Social Change* 34: 183-200.

Whitehead T. 2009. Every phone call, email or website visit 'to be monitored'. *Telegraph.co.uk*, 24 April. Available at: www.telegraph.co.uk/news/uknews/5215413/Every-phone-call-email-or-website-visit-to-be-monitored.html.

Williams, M. 2007. Policing & Cybersociety: The Maturation of Regulation within an Online Community. *Policing & Society* 17(1): 59-82.

Williams, M. 2006. *Virtual Criminal: Crime, Deviance and Regulation Online*, Routledge.

Williams, M. 2003. Virtually Criminal: Deviance, Harm and Regulation within an Online Community. Unpublished doctoral thesis, University of Cardiff, Cardiff.

Wjamesau. 2010. How to Save Second Life in Seven Easy Steps. *Social Times*, 29 July. Available at: socialtimes.com/save-second-life_b18650.

Woodhouse, J. 2010. CCTV and its effectiveness in tackling crime. Home Officer. Available at: www.parliament.uk/briefing-papers/SN05624.pdf.

Yar, M. 2006. *Cybercrime and Society* SAGE Publications.

Zedner, L. 2003. Too Much Security? *International Journal of the Sociology of Law* 31: 155-184.

Zedner, L. 2009. *Security: Key Ideas in Criminology Series*. London and New York: Routledge.