Surveillance & Society

Article

Surveillant Assemblages of Governance in Massively Multiplayer Online Games: A Comparative Analysis

Aphra Kerr
National University of Ireland, Maynooth, Ireland.
Aphra.kerr@nuim.ie

Stefano De Paoli
Abertay University, Scotland.
s.depaoli@abertay.ac.uk

Max Keatinge
Independent Scholar, Ireland.
maxkeatinge@yahoo.co.uk

Abstract

This paper explores governance in Massively Multiplayer Online Games (MMOGs), one sub-sector of the digital games industry. Informed by media governance studies, Surveillance Studies, and game studies, this paper identifies five elements which form part of the system of governance in MMOGs. These elements are: game code and rules; game policies; company community management practices; player participatory practices; and paratexts. Together these governance elements function as a surveillant assemblage, which relies to varying degrees on lateral and hierarchical forms of surveillance, and the assembly of human and non-human elements.

Using qualitative mixed methods we examine and compare how these elements operate in three commercial MMOGs: Eve Online, World of Warcraft and Tibia. While peer and participatory surveillance elements are important, we identified two major trends in the governance of disruptive behaviours by the game companies in our case studies. Firstly, an increasing reliance on automated forms of dataveillance to control and punish game players, and secondly, increasing recourse to contract law and diminishing user privacy rights. Game players found it difficult to appeal the changing terms and conditions and they turned to creating paratexts outside of the game in an attempt to negotiate the boundaries of the surveillant assemblage. In the wider context of self-regulated governance systems these trends highlight the relevance of consumer rights, privacy, and data protection legislation to online games and the usefulness of bringing game studies and Surveillance Studies into dialogue.

Introduction

While studies on internet surveillance focus extensively on search engines and social networking sites (Gillespie 2010; Albrechtslund and Dubbeld 2005; Albrechtslund 2008; Lyon 2006; Fuchs 2011), commercial digital online games remain largely underexplored. Yet digital games are one of the fastest growing entertainment industries worth $60 billion globally (Zackariasson and Wilson 2012) and online games are experiencing the most rapid growth within this (De Prato et al. 2010). The industry is increasingly offering games as a service over the internet and companies need to manage large numbers of players and their devices. Companies use surveillance to both enable and restrict forms of online game play and we believe that game studies has much to learn from Surveillance Studies, and vice versa.

Massively Multiplayer Online Games (MMOGs) are a subset of the online digital games industry. MMOGs are two- and three-dimensional virtual worlds played by thousands of players simultaneously.

Kerr, A., S. De Paoli and M. Keatinge 2014. Surveillant Assemblages of Governance in Massively Multiplayer Online Games: A Comparative Analysis. *Surveillance& Society* 12(3): 320-336.
http://www.surveillance-and-society.org | ISSN: 1477-7487

Players must buy the game and then pay a monthly subscription,[1] or in some cases players freely download the game and pay small payments to progress. MMOGs differ from other online games such as First Person Shooters in terms of their persistence: a player must log into a server to join the game and when they log out the game continues to exist, and other players continue to play (Taylor 2006a; Kerr 2006). Furthermore, MMOGs are subject to periodic updates and expansions. The most popular MMOGs, such as World of Warcraft[2] or Lineage have millions of players across multiple countries and can be very profitable. Many MMOGs emphasise collaboration and players need to partake in 'quests' to advance up 'levels' in the game.

MMOGs offer a relevant field in which to examine forms of 'new surveillance' (Marx 2007). Most MMOGs run on a client-server architecture whereby players' computers (the clients) connect to the game company computers (the servers) via the internet in order to play. In this architecture, the actions that a player executes on her client machine must be communicated back to the server and to other players' computers for the game to function. If a player moves the avatar on the game map by using the mouse, this action, which happens locally on the client, must be communicated back to the server for the actual avatar movement to take place. The client-server architecture generates huge amounts of data flows and rich databases of player and game behaviour. Game companies use this data to survey player activities, tweak the game design, and monetise the game. Some of this data is presented back to the player to inform them of their progress and enable them to plan their gameplay. Much of this data gathering and monitoring is part of running the game as a commercial service.

Surveillance Studies have argued that mechanisms of surveillance and discipline are not necessarily bad, nor is any form of resistance to these necessarily good (Lyon 2006: 5, 11). The collection and use of data by game companies would appear to constitute an organisational or neutral form of surveillance. However, companies may also use automatic monitoring software to prevent and detect certain forms of disruptive behaviour, especially cheating. In MMOGs when general play and player data is combined with monitoring software to identify, categorise, and discipline disruptive behaviour in the context of a self-regulated industry, we see instances of what Fuchs (2011) would call a negative form of dataveillance and the values and goals underpinning the 'panoptic sort' (Gandy 2012) are revealed.

Commercial online game companies promote their games as social spaces for online communities. Players are empowered to play heroes, go on adventures, and become involved in epic fantasy spaces. In game studies, the emergent and playful properties of games are celebrated and the more negative aspects of control, surveillance, and disciplining largely downplayed. Malaby (2007) for example calls MMOGs social artefacts where players have a crucial role in co-producing the game and others have highlighted how players can also produce their own rules and norms (MacCallum-Stewart 2011). Banks (2005) highlights how players can be disruptive and take great pleasure in exploiting the game's structure and design. However, another group of scholars are exploring online games as governing structures that facilitate more contested forms of surveillance (Humphreys 2008, 2009; de Zwart 2009; Whitson 2010). In this paper, we contribute to this developing literature by exploring the governing structures of MMOGs as an emergent surveillant assemblage (Haggerty and Ericson 2000). Like other surveillant assemblages, the MMOGs assemblage 'resides at the intersections of various media that can be connected for diverse purposes' (Haggerty and Ericson 2000: 609). Non-human elements, like computer code and legal documents, are connected to human elements, like players and game masters, in a surveillant assemblage whose properties emerge over time.

[1] All the cases in this paper rely, in the main, on subscription based business models.

[2] This fell to 7.8 million subscribers by the end of 2013 according to an Activision-Blizzard financial statement. See http://investor.activision.com/annuals.cfm

In this paper we review both the literature on media governance and recent work on games governance in MMOGs, with a focus on the connections with surveillance. Based on this review we identify five elements of the surveillant assemblage that are relevant to governance in MMOGs. We then introduce our methodology of qualitative and comparative mixed method case studies of three commercial MMOGs: World of Warcraft (Activision-Blizzard 2004), Eve Online (CCP 2003) and Tibia (CipSoft 1997). In our analysis, we explore how these five elements function in assemblage in order to shape the governance of online communities in our case studies. Our findings show a tendency for game companies to move towards more hierarchical and legalistic forms of governance and less transparent forms of automated dataveillance. In our conclusion we explore the implications of these findings.

Media Governance and Surveillant Assemblages

In *Surveiller et punir* (1977), Foucault's focus was on the design and creation of technologies of surveillance/visibility, on how they classify and produce discipline. His work is a necessary staring point to discuss diffuse forms of government and performative approaches to power. Indeed if the reader shifts focus away from techniques of visibility and onto techniques of ordering and control, Foucault's work is relevant for media and games research (Simon 2005; Silverman and Simon 2009). His later work also explores the rationalities and moralities involved in government and the potential for resistance. Inspired by Foucault, Dean defines government as:

> any more or less calculated and rational activity, undertaken by a multiplicity of authorities and agencies, employing a variety of techniques and forms of knowledge, that *seeks to shape conduct* by working through our desires, aspirations, interests, and beliefs, for definite but shifting ends and with a diverse set of relatively unpredictable consequences, effects and outcomes.
>
> (Dean 1999: 11)

Governance as a term in policy discourse emerged recently and coincided with an intense period of liberalisation of media regulation in Western Europe in line with earlier changes in North America. While governance as a concept may have specific meanings in cognate disciplines like economics or political science, in the context of media policy the concept is used to analyse multimodal regulation (e.g. statutory, co-regulation, and self-regulation) that operates at multiple levels (e.g. local, regional, and global) across multiple dimensions (Puppis 2010). More recently, the concept of governance has been applied to networked systems of regulation in new media (Curran et al. 2012: 98). In self-regulated media industries, the state, or in some cases a supra-national body, develops a broad governance framework but delegates the actual government of media production and practice to media organisations.

Existing work on new media governance highlights the role played by non-human actors like hardware and software (Lessig 1996) and in Science and Technology Studies the agency of non-human actors is widely debated (Akrich 1995; Oudshoorn and Pinch 2008). Braman and Malaby (2006) note that 'technical decisions' implicitly structure social relations and have anticipated and unanticipated effects. Introna and Wood (2004) have written about algorithmic surveillance, a process in which algorithms (for example, for automatic facial recognition) enact political decisions, which are part of the technical design. Far from being neutral carriers, therefore algorithms can embody and enact political and economic values and goals connected with surveillance.

With the increasing ability of digital technologies to gather big data, it is the ability to process and interpret this data which today extends their surveillance power. New concepts have been forged to understand this development. Both De Landa (2001) and Braman (2006) develop the 'panspectron' concept, defined as 'how information is gathered about everything, all the time, and particular subjects become visible only in response to the asking of a question' (Braman 2006: 315). The panspectron

monitors every possible action of the actors and deviant behaviour is identified by querying the data. Gandy has explored how automated systems generate transaction data that can be automatically mined in ways that both improve and undermine the quality of service we receive. For Gandy (2012), it is the values underpinning this discrimination that should concern us. For us, certain aspects of MMOGs are examples of panspectrons, which are justified by economic goals and values which emphasise a very limited view of 'quality of service' and 'community'. They are assemblages of techniques that embrace mass, self, and participatory dataveillance (Fuchs 2011).

A key concept for our research is the surveillant assemblage (Haggerty and Ericson 2000). Relying on the work by Deleuze and Guattari (1987), and their notion of assemblage, Haggerty and Ericson developed a concept that accounts for the process of convergence of diverse discrete systems into a seamless surveillant whole. The concept of assemblage (Deleuze and Guattari 1987) emphasises the idea that a phenomenon should be conceptualised as the dynamic result of the empirical and historical formation of relations among a disperse variety elements, rather than via the description of essential property of discrete elements. The general concept of assemblage has previously been applied to digital games (Karppi and Sotamaa 2012) and MMOGs (De Paoli and Kerr 2010; Taylor 2009) with a focus on the emergent properties of games.

Haggerty and Ericson (2000: 610) emphasise that surveillance should be conceptualised as the coalescence of a variety of heterogeneous elements—a surveillant assemblage: 'The analysis of surveillance tends to focus on the capabilities of a number of discrete technologies or social practices. Analysts typically highlight the proliferation of such phenomena and emphasize how they cumulatively pose a threat to civil liberties'. Therefore rather than focusing on discrete capabilities of, for example, CCTV cameras as an unitary technology, the focus is on understanding how CCTVs are 'an assemblage that aligns computers, cameras, people and telecommunications in order to survey the public streets' (Haggerty and Ericson 2000: 614).

The concept of surveillant assemblage helps to focus our research inquiry on the interrelation of a variety of MMOGs elements (that range from computer code, architecture, policy documents and companies to player practices) and the emergent properties of government. Also, this concept does not foreclose the observations of resistant player activities and how these activities function with other elements of the assemblage, for example the subversion of code.

Surveillant Assemblages in Governance of Digital Games

Current research on game governance tends to focus on the micro game world. One strand focuses on the game developer. Tschang and Comas (2010) identify three approaches to designing virtual worlds: designer as god, user generated and economically rational. The 'designer as god' approach appears to dominate. Castronova (2005: 208) argues that companies are the 'coding authority' in MMOGs and act as 'tyrant gods' with End User License Agreements (EULAs) as their 'diktats'. He suggests there is little economic incentive for MMOGs to invest in improving governance structures, given the switching costs involved in moving from game to game. Bartle (2006) agrees and argues that game publishers act more like deities than governments. More than a decade ago, game designer Raph Koster (2000) asserted that while the sovereignty of the gameworld rests with the producer, players nevertheless have the 'right to know and demand the enforcement of the standards by which (they) use this power'.

Other work focuses more on the relationship between the game developers and players. de Zwart (2009) identifies three mechanisms of governance in MMOGs: EULAs and policy documents, game code, and player norms. She also identifies three key stakeholders: real world governments, game/platform developers, and players. She notes that conflicts arise between platform developers and players, between players and other players, and between platform developers and third party copyright owners. Humphreys

(2008, 2009) adds company 'practices of community management' and highlights how governance practices often work though informal knowledge, language, and identities as well as through formal documents and institutions. In both de Zwart and Humphreys we see examples of how player practices and community norms have a role in MMOG governance and how players develop and deploy technologies to improve their gameplay experience. Elsewhere others have documented how players develop their own sociotechnical systems to improve and rationalise gameplay in MMOGs (Silverman and Simon 2009; Taylor 2006a, 2006b, 2006c).

de Zwart (2009) argues that as MMOGs grow in size and operate across multiple markets and servers, managing or governing the community for game companies becomes more difficult and expensive. Companies are looking to software code, stricter policy documents and non-human alternatives to govern their complex online services. For example, EULAs are increasingly legalistic and while many of the clauses may not be implemented, they nevertheless exist as the basis of potential sanction. MMOGs are where, according to Coleman and Dyer-Witheford (2007: 943), the 'most complex encounters between commons and corporate play regimes' take place. Two key aspects emerge from our literature review: players participate in numerous ways in MMOG governance and surveillance, and broader contextual and jurisdictional issues are increasing in importance (Taylor 2006c).

Our research builds upon the aforementioned work but based on our case studies we not only expand the range of elements, we also analyse how they function in an assemblage. The emergent relations between these diverse governance elements form a 'local' surveillant assemblage of a game which is situated within a wider social, political and legal context. The elements are:

1. Game architecture, software code and game rules;
2. Policy Documents—e.g. EULAs, Codes of Conduct and legal documents;
3. Company community management practices;
4. Peer and participatory surveillance between players, community norms;
5. Paratexts—e.g. company produced—game packaging, cheat guides, official websites, leader boards, and forums; player produced—game content mods and player websites.

Based on our case studies we added paratexts as a fifth element of governance in MMOGs. This is a concept developed by Genette in relation to literature but refers to everything that informs, or relates to, a given text, yet is not strictly part of it (1987/1997: 5). Paratexts influence how a text is perceived and shapes the meaning it conveys. Writing about literature, Genette distinguishes between peritexts—elements within the text like the preface and titles—and epitexts—elements outside of the text like reviews and interviews. Lunenfeld (2000: 15) applied the concept in relation to digital media and Gray (2010) in relation to film and television (e.g. fan videos). Consalvo (2007) uses the concept of paratext in her discussion of commercially-produced cheating guides for digital games. Some player-produced paratexts are encouraged by game producers, and some are not. We found that paratexts, especially epitexts, were an important source of contention between developers and players and a space where players enact participatory surveillance.

Methodology

This paper is based on multi-method qualitative studies of various lengths involving analysis of gameplay, game documents, player interviews, and analysis of player communications between 2008 and 2011**.** This paper explores governance practices in World of Warcraft (WoW), Eve Online (Eve), and Tibia whose headquarters are based in the USA, Iceland, and Germany respectively. These games were chosen because the developers are located in three different legal jurisdictions, they had different sized player populations, and they had different design structures. Table 1 summarises the key characteristics of our case studies.

	Case 1	**Case 2**	**Case 3**
	WoW	***Eve***	***Tibia***
Year founded	2004	2003	1997
Country headquarters	USA	Iceland	Germany
Numbers of active subscriptions worldwide (from mmogcharts.com for 2010)[3]	12,000,000	450,000	100,000
Basic Design	Medieval fantasy, 3D, players can collaborate in 'quests' and progress through levels.	Science- fiction set in space, 3D, anarchic, players can form 'alliances' and join 'corporations'	Fantasy, 2D, no sound Players can collaborate on 'quests'[4] and in 'guilds'[5]
Rating in Europe	PEGI 12 + depictions of violence + bad language	PEGI 12 + depictions of violence	Not officially rated Marketed as 12+

Table 1: *Overview of Case Studies (at the time of the fieldwork).*

The first stage of our project involved two month-long participant observations in WoW and Eve in 2008. The researcher played on WoW's 'Frostmane' server and Eve's 'Tranquillity' server cluster. Additional data was gathered from chat logs and game documents. During the observation the researcher joined player-run organisations to observe and participate in their activities. We informed gatekeepers in the game about the research and they facilitated it. Gatekeepers helped to identify and specify the different mechanisms of governance that operated.

The second stage of our project involved a longitudinal study of an anti-cheating campaign in one game. The Tibia case study was conducted between January 2009 and June 2010 and used participant observation and online archival research.[6] The core of the data came from threads on the official Tibia forums (1485 forum pages consisting of 20 posts each), where players and the company discussed cheating, especially the use of software robots known as 'bots'. The data collection also included official game policy documents and playing the game with two different characters/avatars. This case enabled the team to explore longitudinally how an MMOG deployed its governance elements with regard to cheating.

Bots are computer programs that are used to automate repetitive gameplay activities and provide a shortcut to levelling up. Levelling is a key activity for MMOG players, which often entails an array of repetitive time-consuming actions. This entails strengthening the abilities, skills and experience of an avatar. Bots are defined as cheating in MMOGs because they alter the equilibrium of a game, for example its economy and level system (Yan and Choi 2002; Yan and Randell 2005). In most MMOGs—and Tibia makes no exception—using a bot is an explicit violation of game policies and the developer/player

[3] See http://mmodata.net/ for updated figures. These figures may vary from those published by the companies.

[4] Game quests are common in role-playing games, including digital games, and they include a mission or a challenge that a player or a group of players (guild) can complete in order to obtain a specific reward.

[5] Guilds are organised groups of players that share some goals and that together can complete game quests or engage in alliances or wars with other organised groups or guilds. Guilds are usually composed of characters with different roles and abilities.

[6] We follow NUI Maynooth research policies and the Association of Internet Research Ethical Guidelines.

contract.In January 2009, CipSoft launched an anti-cheating campaign to prevent the use of bots in Tibia and a number of changes were introduced which deeply affected the surveillant assemblage.

Finally, five semi-structured interviews were conducted in 2012 and 2013 with representatives from the publisher's representative body in Europe, the Interactive Software Federation of Europe (ISFE), and companies providing MMOG service and community support, localisation and marketing.

Surveillance Assemblages at Work

In the following section we outline and compare the surveillant assemblage of the three case studies. We focus in particular on the tension between the desire of the game companies to maintain an efficient, secure, and cost effective governance structure and the activities that some players engage in to subvert this.

Game Architecture, Software Code and Game Rules

Eve, WoW, and Tibia use a client/server architecture, although Eve players all compete in a single world of connected servers while WoW and Tibia players can choose particular servers based on different locations or rule sets. Further, the games differ in their basic design with Eve having a more emergent design with multiple variations compared to WoW and Tibia, which have a more progressive and pre-defined set of actions (Juul 2002; Keatinge 2010).

There were numerous examples during our fieldwork of the 'emergent' properties of Eve and instances where software code and rule changes were exploited by players in unanticipated ways. These situations forced the game company to intervene by introducing changes and reconfiguring the surveillant assemblage. For example, the 'Pew-Pew Palooza' incident was staged by a group of players called the 'Privateer alliance'.[7]By applying Eve's rules for declaring war in an unconventional manner they successfully turned a relatively safe haven in the game world into a warzone. Within a month, the company introduced a new piece of code to alter the game rules and prevent such incidents. A further example was staged in Eve by a group of players called '4S'. When the designers introduced a new class of ship—the 4S—players discovered that they could jettison thousands of 'space shuttles' in Jita and crash the server, forcefully disconnecting all players in it. At this time there were no rules to prevent this. These examples demonstrate how players can exploit game rules for their own pleasure and how developers are forced to reconfigure several aspects of the assemblage such as game code or rules to subvert these activities and maintain both the quality of their service and a strict governance.

While most software and code contributes to the creation of the game, anti-cheating tools are another type of software that automatically enforce the EULAs or the Terms of Service of a game. WoW, for example, has *the Warden,* a monitoring tool which scans the RAM of player computers (the clients) searching for cheating programs. The Warden is an example of a panspectron: it gathers information about all the programs executed on the client of all players and it compares these programs with a database of known cheating codes which are maintained by the game company. Therefore while information is collected on all the players, cheating behaviour is identified by asking specific questions (i.e. comparing the programs on client computers with known cheating code). Anti-cheating tools are therefore intrusive technologies because they collect data from each of the players' computers, even if a player is not a cheater.

In Tibia an anti-cheating tool was introduced during our fieldwork in order to detect the use of bots. The introduction of this new anti-cheating tool triggered a clear alteration of the existing surveillant

[7] The rules of Eve allow avatars to band together into organisations called 'corporations'. Corporations can have from less than ten avatars to several hundred members. 'Alliances' are groups of corporations.

assemblage with a consequent reshaping of the game governance. The following article from January 2010 states:

> a huge amount of data about cheaters in Tibia has been collected, analysed, evaluated and re-evaluated. Only recently, this whole process has reached a point when sufficient statistical information was accumulated which allowed to draw comprehensive and truly reliable conclusions about the cheating situation, and to plan our next strategic steps.
>
> (CipSoft 2010a)

Data gathered by the tool was used to improve its effectiveness and strengthen the company's anti-cheating strategy. This tool is another panspectron, a technology that systematically collects data on player activities and analyses it for purposes of surveillance and monitoring. From January 2009, bans for the use of bots were instigated by CipSoft. A 'ban' is a type of punishment that means that a player's account is temporary excluded from the game. In the case of cheating by using bots, the standard ban is one month. With the anti-cheating tool, bans were automatically made based on results coming from the decision process of the panspectron tool but the operation and accuracy of the anti-cheating tool was far from transparent for players. The company suggested that machine detections were more accurate than human detection and they stated in public forum posts that complaining about the process was in vain (CipSoft 2009b):

> Today we have punished 5163 Tibia accounts for using unofficial software to play …. These accounts have been identified by our automatic tool. For this reason, complaints about these punishments are in vain.

The key governance issue is that players were not able to appeal to the panspectron machine if they thought that the ban was unfair.

Policy Documents

Self-regulation is the dominant mode of governance of the games industry in North America and Europe. In the European context game companies are largely free to set their own rules within a game as long as they conform to the broader legal frameworks dealing with protection of minors, data protection, privacy, and intellectual property. Game players enter into a private contractual agreement with the companies that falls within general consumer rights law (Lastowska 2010).

In our interviews it became apparent that new modes of co-regulation and new national policies have emerged which impinge upon online games. In an attempt to overcome national variations there has been a push by the games industry to develop pan-European regulations. One such example is the Pan European Game Information (PEGI) age and content rating system which is partly funded by the European Commission, was developed by the Interactive Software Federation of Europe (ISFE), and is run and monitored by a third party. This was recently extended to cover online games.[8] Both WoW and Eve are officially rated 12+ using PEGI online while Tibia is positioned as a 12+ game.

ISFE is the representative body for major game publishers in Europe. With the Council of Europe it co-published a voluntary code in 2008 outlining the roles and responsibilities of online game providers, especially in relation to excessive use and harmful content (Council of Europe 2008).The guidelines encourage the development of reporting systems for players to report illegal or harmful content or

[8] See http://www.pegionline.eu/en/index/. The games examined in this paper are all categorised as PEGI 12—'Videogames that show violence of a slightly more graphic nature towards fantasy character and/or non graphic violence towards human-looking characters or recognisable animals, as well as videogames that show nudity of a slightly more graphic nature would fall in this age category. Any bad language in this category must be mild and fall short of sexual expletives'.

behaviour, but stops short of mandating them. Some consideration is given to the risks to player privacy of exchanging personal data online and the rights of players with regard to user produced content. All three cases that we examined had some form of reporting system to game masters but variations were found in relation to player privacy and user generated content.

One interviewee noted that ISFE (2012) had concerns with draft EU data protection legislation. In particular they highlighted the proposed definition of personal data, data portability and the balance between the right to privacy and the right to property, in particular intellectual property. These concerns signal that digital games, and especially online games, are an important arena where legal and policy decisions at EU level will have an impact. ISFE has joined with a number of other digital media associations in Europe to form the 'Industry Coalition for Data Protection' to lobby on these issues (ISFE 2010). These examples also point to an on-going process of supranational institutional and regulatory development in Europe in addition to existing national regulations (e.g. USK in Germany) and company policies.

Where we see the broader supra-national laws and codes of conduct intersect with particular online games is in the EULAs, codes of conduct, and similar policies that seek to explicitly govern the conduct of players. Legal terms of services or software are a form of inscription: textual technologies that prescribe actions for users and that are often related to copyright or other laws such as privacy laws (De Paoli et al. 2008). These documents are hierarchical and exercised almost exclusively by developers or publishers. These are governing documents for players and they function in assemblage with other elements. For example, they work with the software to regulate how the game is used or with other paratexts, such as game forums, to forbid the use of real names while posting. The only agency players possess to negotiate the EULA presented to them when they log into the games initially is to refuse, and consequently be barred from the gameworld. Like code therefore legal documents have a prescriptive nature with a focus on governing behaviour, defining violations, and punishments (De Paoli and Kerr 2012).

Some policy documents for instance forbid commercial exploitation of modifications created by players and in some cases set requirements as to the type of content that can be developed. This is an example of how software and legal documents functions as assemblage. However software is a flexible technology and with simple tools it is possible even for non-programmers to produce modifications and modifying the game content is a common practice (Nieborg and van der Graaf 2008). In our study there were differences between the documents governing the MMOGs and in the ability and desire of the publishers/developers to enforce them. For example, the legal documents of WoW and Eve both explicitly forbid the development of third party software that might modify the game:

> You will not attempt to decipher, hack into or interfere with any transmissions to or from the EVE Online servers, nor will you try to create or use any third party add-ons, extras or tools for the game...
>
> (Eve, Online Terms of Service, CCP 2008)

> [users are prohibited to]...(1) modify or cause to be modified any files that are a part of a World of Warcraft installation; (2) create or use cheats, 'mods', and/or hacks, or any other third-party software designed to modify the World of Warcraft experience; (3) use any third-party software that intercepts, 'mines', or otherwise collects information from or through World of Warcraft...
>
> (WoW Terms of Use, Activision-Blizzard 2009)[9]

[9] Since our fieldwork, WoW's Terms of Service have changed.

However, player-created modifications are regulated differently in Eve and WoW. WoW's Application Programming Interface (API) affords users easy modification of select parts of WoW's interface. WoW's terms of use and its API are part of an assemblage that players may leverage to re-inscribe their vision in WoW, for example in the form of modified avatars. In Eve the assemblage of legal terms and code is much stricter and the space that players have for changing the design is limited. The differences between the two game governance regimes are visible here and mean that there are a vast number of interface modifications developed and maintained by WoW players, but these are largely absent in Eve.

In the case of Tibia, our research on policy documents focussed on cheating and the introduction of the anti-cheating tool. Some players welcomed the tool stating that it was necessary to stop bots in Tibia. They were willing to give away some control over their data in exchange for a solution to cheating. However, others felt that monitoring a player's computer is a form of surveillance and an invasion of privacy. On the forums they questioned the lack of transparency around the data collection made by the anti-cheating tool. Others expressed concerns and suggested that players were being asked to surrender too much privacy to the company: 'I would never play a Tibia again, if they did spy on what programs I am using'[Character Misericordiae, 14/01/2009, Post #21854869].[10]

A few months after the launch of the new anti-cheating campaign CipSoft introduced a change in the game's Privacy Policy (PP). Changes included provisions extending the data being collected by the company; stating that the company can use data about the users to conduct marketing actions; stating that the company can pass this data on to third parties in order to produce anonymous statistics; and finally a change to the rules upon which this new PP could be accepted by the players. For players the only way they could resist the new PP was to opt-out and consequently ceasing to play the game. New legal inscriptions were therefore put in place by the company. Not all these changes relate with the operations of the anti-cheating tool—but some do—and furthermore these changes were unilaterally introduced and had significant implications for the governance of the game. Changes to paragraph 2 of the PP seem to be the most relevant for our discussion:

> The type of usage data that we store has now been extended to include data about hardware and software of the user's computer system. We will mainly use this data for anonymous statistical surveys, for error analysis and the optimisation of our services.
>
> (CipSoft 2009a)

This new provision added data about hardware and software on users' computers to previously recorded data including the 'IP address, browser version, access time, information on the type and the aim of requests'. For many on the forums this was an explicit declaration that the new anti-cheating tool was collecting data on their computers. Elsewhere we have described a similar provision of the WoW's EULA, known as the 'consent to monitor', which grants the game company the right to monitor what is happening on the player's computer (De Paoli and Kerr 2010). Collecting data about the hardware and software of the player's computer, in the case of Tibia, is another case of 'consent to monitor'. This is another example of the unstable and reconfigurable status of the surveillant assemblage; with a modification of the relations between the company and the player (from the old to the new PP) which is inscribed not only in the code of the game (i.e. monitoring tool), but also in the legal documents that allows the monitoring tool to collect data.

In all our cases the policy documents—which the players accept when they create an account—state that the company can introduce unilateral changes to their policy documents. In the Tibia documents it states

[10] Tibia forum posts are formatted as [character name, number of post, date]. There is no URL for this data as old discussions are periodically removed from the website.

that the company has the right to revise the terms of any legal documents, at their discretion. Some Tibia players supported this right:

> I highly doubt CIP will use the info for anything inappropriate. Why would they do that? If it was proven they sold the info, or somehow abused our trust they would lose their costumers and have to look for a new job quite soon! ... Keep up the good work CIP! And do whatever it takes to make this game as good as possible for the honest players =)
> [Character Forsaken Damien, Post #22675601, 23/03/2009]

Others disagree:

> This should be called the 'no privacy policy', because it appears that Tibia players won't be getting any. This is something, I'm sure, people are not going to be happy about.
> [Character Walk, Post #22671232, 23/03/2009]

What is clear is the company's practice of making unilateral decisions in a hierarchical way. Furthermore, this practice connects with the surveillant assemblage composed of elements such as anti-cheating tools, policy documents, company decisions and player activities. This assemblage is a shifting process of governance, which in the specific example served to answer to the disruption caused by cheating.

Company Community Management Practices

WoW, Eve, and Tibia employ community managers to oversee game players, monitor behaviour in games, and provide feedback to game developers. Community management practices function in assemblage with, for example, policy documents, the game code, and paratexts such as official blogs and forum posts. All these elements define 'rules violations' or 'good behaviour'. Furthermore, given the size of the game worlds, these managers also rely on game players—as a component of the assemblage—to report issues in the game and to help monitor the game world. For example, CCP mobilises players to help counteract a real-money-trade (RMT) related problem, i.e. the exchange of property, avatars, or accounts in MMOGs for real-world currency. RMT is an activity which is explicitly forbidden by the game EULA section 6.b (CCP 2012a):

> You may not transfer, sell or auction, or buy or accept any offer to transfer, sell or auction (or offer to do any of the foregoing), any content appearing within the Game environment, including without limitation characters, character attributes, items, currency, and objects, other than via a permitted character.

Players who wished to report RMT to community managers used in-game reporting tools, direct email or requested in-game support directly to Game Masters. Game forums are used by community managers to suggest these forms of lateral surveillance.[11] This is further reinforced by the use of paratexts such as official blogs (CCP 2012b) that explain what the company does for counteracting RMT and the penalties for violating the rule.[12] Community managers also encourage the 'good' conduct of those who refuse to engage in the practice. This underlying governmentality suggests that self-regulation and lateral surveillance of RMT—for example by means of reporting—improves the state of Eve for all 'good players':

[11] See for example a forum discussion here: https://forums.eveonline.com/default.aspx?g=posts&m=2113657

[12] Just after our fieldwork CCP introduced a Council of Stellar Management and annual elections of player representatives. A statement on player rights added a degree of collaborative governance to their structures.

> ...this will not be possible without help from you, th(e) players. The demand for ISK is what keeps the RMT element alive. They'll keep coming back as long as players are willing to do business with them.
>
> ['Game Master Grimmi' 2009]

In our cases players were kept from direct involvement in defining key problems or the solutions to fix them. In Tibia community management practices and the request for players to participate to surveillance processes changed with the introduction of the monitoring software. Traditionally, Tibia identified botters based on player reports which were then investigated by 'game masters' (GMs). During our fieldwork GMs were experienced players who volunteered to assist CipSoft in monitoring and punishing rule violations. GMs were therefore players co-opted into the community management and monitoring process. Player reporting on bots in Tibia was a form of community management practice coupled with the judgement of GMs. The introduction of the anti-cheating tool brought an organisational change:

> you don't need to report botters to GMs any longer since our automatic tool is now active and running. GMs can now focus on other rule violations.
>
> [Community Manager Mirade, 03/02/2009, Post #22076329]

The introduction of a new technology removed the need for player reporting within the game, at least in relation to the issue of bots and cheating. The message from the company states that reporting the use of bots is not necessary anymore but that players can continue reporting other game violations to GMs (e.g. use of bad language). This removed explicit 'human judgment on cheating'. This is not to state that human mediated anti-cheating processes were more accurate. Indeed, many players had concerns about ban judgements taken by GMs who were accused of being biased. Instead, the values, biases, and intentions which are coded into, and develop over time, in the anti-cheating tool are not seen as biased. Interestingly, in August 2010, CipSoft announced that due to the new enforcement strategies and the use of monitoring tools the existence of volunteers GMs were not necessary anymore for the game (CipSoft 2010b). By introducing an anti-cheating tool CipSoft has redefined the composition of the surveillant assemblage: rules (policy documents) are enforced by software code (the anti-cheating tool) and the role of peer-surveillance within the assemblage is greatly diminished.

Peer and Participatory Surveillance and Player-Produced Paratexts

Previous work has pointed to the important role of community norms and player developed rules within MMOGs (Humphreys 2008, 2009; de Zwart 2009). These elements function in assemblage with other governance elements and in our cases an interesting example is the practice of 'spying' on other players or guilds. We found that 'spying' as a gameplay strategy was not explicitly forbidden by the coded rules of either Eve or WoW but nevertheless the rules and architecture of the former encouraged it. Spies can have far-reaching effects in Eve; particularly successful players may steal the entirety of a 'corporation's' assets or even disband it, should they gain access to certain information. Williams et al. (2006: 350) note that in contrast the practice is less common in WoW:

> Less common were intra-guild intrigues such as spies placed inside another organization, the poaching of top players, shared chat channels between guilds, and the occasional rivalry—but because the game mechanics do not allow for much intra-faction conflict, these rivalries rarely mattered.

As spying can be used to greater effect in Eve compared to WoW, it is unsurprising that modes of game play revolving around it are more common. However, this contrast between WoW and Eve indicates that coded rules, even when they do not directly prescribe action, still preconfigure player-negotiated practices of governance in MMOGs. It is also an interesting example of surveillance as play, or as part of play in online games.

Our research indicates that another relevant element of the surveillant assemblage and of participatory surveillance are paratexts. So far we have mainly discussed official paratexts such as blogs made by companies and community managers. While it is difficult to map paratext development by game players about a game world that exists on multiple servers we found many examples of rich player productivity through paratexts, including killboards and player websites. Many of Eve's paratexts did not directly intervene in the game environment given the rules in its policy documents, but their existence demonstrates that for many players part of the pleasure of a game is creating paratexts about, and for, the game.

A number of the player-created paratexts were directly connected with participatory surveillance and some were sanctioned by the game companies. In Eve, for example, killboards involved participatory surveillance and some were officially sanctioned by CCP. Killboards are epitexts developed by game players and consist of an e-mail which lists the details of a fight, and is sent to the victim and victor of a given combat. Killmails can be used to construct a public record if players upload them to public killboards. Battleclinic's killboard service, Griefwatch (http://www.griefwatch.net/), is one example. The site is self-described as an 'award-winning independent game support site' devoted to several games, including Eve, whose members 'build publisher-sanctioned tools and guides and provide these free to players' (http://www.Battleclinic.com). Through killmails voluntarily supplied by players, Griefwatch makes public information which would ordinarily not be publicly available, and transforms it into a durable and widely accessible paratext. It provides a partial alternative way of constructing 'good players' and 'game history'. This player data gathering and epitext provides a way for players to survey the tactics of other players. However, the control that killboards provide to players is contingent upon the information supplied being correct—mails can be faked, or individual players can simply opt to not use them.

In Tibia we encountered player paratexts which were designed to monitor cheating activities. These paratexts were unofficial and not embedded in the official game management. One example was player-created websites that monitor the online time of Tibia characters. Since bots are computer programs, they can play for extended periods without getting tired. This means that a character controlled by a bot could have long online times of almost 24 hours a day for weeks. It is possible with some basic computing skills to read the online time of individual characters from the official Tibia website and aggregate them in intelligible lists, in order to identify characters whose play time seem unhuman. These characters are called 'insomniacs' by the Tibia community. At the time of our investigation there was a website called Pskonejott (2006-2009) that was providing online times in order to identify 'insomniacs':

> The online time counter was programmed to help in locating players that either use bots/macros, or character share to remain in game for very large amounts of time. Although the online time counter may give a good indication that someone is violating the rules in this way, it is only an indication.

While some players may enjoy playing for extended periods, the idea of websites such as pskonejott is that monitoring online time could give at least an indication if a character is controlled by a bot, or if it is shared by many players (another form of cheating). More recently, another website called guildstats offers online times and the identification of insomniacs (see http://www.guildstats.eu/time-onlineEntries). Table 2 presents a recent example of a partial table of an insomniac entry for a Tibia character taken from Guildstats (2014).

In Table 2 (overleaf) we can observe the date of the entry and the online times. In a couple of cases we have long daily online times (between 21 and 24 hours) for 4-5 days in a row (e.g. from 31/01/2014 – 04/02/2014). This extended online time is a type of behaviour that might be a sign of use of bots, as it is difficult for a single human player to sustain such long periods of play. While information like this may

only be used as reference (it is not possible for us to state what actions were taken based on this information), it shows how players produce paratexts that feed into a lateral surveillance process and form part of the surveillant assemblage of MMOGs.

Date	Online Time
25-01-2014	21h 15min
27-01-2014	23h 15min
28-01-2014	23h 30min
31-01-2014	23h 15min
01-02-2014	22h 45min
02-02-2014	23h 15min
03-02-2014	23h
04-02-2014	23h 45min
07-02-2014	21h
09-02-2014	23h

Table 2.*An insomniac entry from a player-produced monitoring website*

Conclusion

A core contribution of this paper is to bring together the concepts of media and game governance with surveillant assemblages and to demonstrate how governance and surveillance operate in the regulation of MMOGs. These assemblages demonstrate that game governance by companies responds to, and shapes the behaviour of players but is often in flux, shifting and adjusting (Whitson 2010; Zabban 2011). In this paper we examined the surveillant assemblages of MMOGs composed of diverse elements and tracing how their inter-relations and the changes in these relations shape the governance of MMOGs. Company game architecture, code, policies, and paratexts were hierarchical (even if sometimes driven by player behaviour) and appealed to multiple levels of state and regional regulatory and legal systems. At the same time community management, peer and participatory surveillance, and player-produced paratexts involved significant player participation and lateral surveillance. We also found examples of playful surveillance by players within games (e.g. spying). Paratexts are a significant element of the assemblage where governance is explained, in the case of game company's official paratexts (e.g. blogs or articles,) and where players and third parties collaborate and negotiate hierarchical game governance outside the direct control of companies, as in the example of the killboard or insomniac tables. In some cases game companies have started to approve player sites in an attempt to monitor them more closely.

A practice which is considered disruptive and can alter the stability of a surveillant assemblage in MMOGs is cheating and in particular cheating using bots. Cheating is legally and morally ambiguous in MMOGs but is not a crime (Kimppa and Bisset 2005; Consalvo 2007; De Paoli and Kerr 2010; Kücklich 2009; Bakioglu 2012). An important trend, which occurred during our fieldwork, is the shift in the governance of cheating using bots from player reporting and game masters to automatic surveillance by digital technologies and the use of policy documents and privacy rules to support this change.

Anti-cheating tools identify cheating avatars and accounts as defined by game companies in their policy documents. They gather data about everything and query it using an evolving set of deviant behavioural patterns to take action to identify and punish players who cheat using bots. While this process was largely invisible to players and researchers, its existence was declared by the companies on public forums. This was justified with a discourse of security and fair play and anti-cheating tools' existence was publicised, in our opinion, to discipline the conduct of players and encourage acceptable behaviour. The resistant possibilities for players in relation to this tool were limited. Some players accepted the changes. Some players threatened to leave the game. Others employed companies to develop new code to circumvent the regulations. The fact that there is a continuous need to monitor the use of bots by players suggests that some players continue to bot despite the new governance regime.

Of concern here is not the right of game companies to police their games or to define acceptable behaviour. What we are concerned with are the methods used, their lack of visibility, and the implications. The shift from players and game masters to anti-cheating tools that scan player machines introduces less transparent and more hierarchical forms of surveillance. They are an example of new surveillance technologies and they are not neutral. This type of code is a designed agent and bears the biases of its designers. This is an example of algorithmic surveillance (Introna and Wood 2004; Gillespie 2014) and introduces what Van Dijk (2006: 114) calls issues of 'informational privacy'. It is not surprising that industry associations like ISFE and ICDP are concerned that new EU data protection legislation might impose new restrictions on what game companies can do with player data.

As with all communities the levels of transparency, the behaviour of governing agents and the punishments which are enacted are good indications as to the values being fostered. There is a tension in MMOGs between the commercial need for paying players and the banning of paying players from the community. Since we conducted our fieldwork we note that Eve has introduced a democratically elected player council to mediate on game design issues with the games company and other companies have introduced new ways for players to become involved in reporting or adjudicating on disruptive behaviours. These deserve attention but they do not undermine our finding that certain actions taken by game companies are not transparent and may indeed infringe on the consumer rights of their players (i.e. the right of appeal). This was regardless of the legal jurisdiction that the game companies appealed to in their policy documents.

Our research found that despite the existence of participatory surveillance elements in MMOGs, which can be empowering and playful, automatic tools of hierarchical governance are being used to undermine this empowerment. Commercial and security goals are in some instances used to override local consumer and citizen rights and technologies are portrayed as an unbiased mediator. This leads us to argue that MMOGs are more than trivial pastimes. They should be an important site of research for Surveillance Studies as they undermine the dualism of participatory or hierarchical surveillance and provide a fertile field for studies of commercial transnational data gathering and use. We also suggest that longitudinal and comparative studies can help to overcome the significant methodological challenges posed by the lack of visibility of non-human actors in these online worlds and the dynamism and porosity of media 'texts'. Intriguingly for us, as media governance more generally moves away from statutory and hierarchical government, our virtual worlds appear to be embracing it.

Acknowledgements

The authors wish to acknowledge the support of the Irish Higher Education Authority under the PRTLI 4 programme, our research participants and the helpful advice of our reviewers.

References

Activision-Blizzard. 2004. *World of Warcraft*. California: Blizzard Entertainment.

Activision-Blizzard. 2009. *World of Warcraft Terms of Use.* California: Blizzard Entertainment. Available at http://us.blizzard.com/en-us/company/legal/wow_tou.html

Akrich, Madeleine. 1995. User Representations: Practices, Methods and Sociology. In: *Managing Technology in Society*, eds Arie Rip, Thomas Misa and Schot Johan, 167-184. London: Pinter.

Albrechtslund, Anders. 2008. Online Social Networking as Participatory Surveillance. *First Monday* 13 (3). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/2142 (last accessed 18 May 2014).

Albrechtslund, Anders, and Lynsey Dubbeld. 2005. The Plays and Arts of Surveillance: Studying Surveillance as Entertainment. *Surveillance & Society* 3 (2/3): 216-221.

Bakioglu, Burcu. 2012. Negotiating Governance in Virtual Worlds: Grief Play, Hacktivism, and LeakOps in Second Life. *New Review of Hypermedia and Multimedia* 18(4): 237-259.

Banks, John. 2005. Opening the Production Pipeline: Unruly Creators. In *Worlds in Play: International Perspectives on Digital Games Research,* eds Suzanne de Castell and Jennifer Jenson, 143-150. Vancouver: DiGRA and Simon Fraser University.

Bartle, Richard, A. 2006. Why Governments aren't Gods and Gods aren't Governments. *First Monday* 11 (7) doi:10.5210/fm.v0i0.1613

Braman, Sandra. 2006. Tactical Memory: The Politics of Openness in the Construction of Memory. *First Monday* 11(7) doi:10.5210/fm.v11i7.1363
Braman, Sandra, and Thomas Malaby. 2006. Preface. *First Monday* 11 (7) doi:10.5210/fm.v0i0.1605
Castronova, Edward. 2005. *Synthetic Worlds. The Business and Culture of Online Games*. Chicago: University of Chicago Press.
CCP. 2003. *Eve Online*. Reykjavík: CCP. Available at http://www.eveonline.com/
CCP. 2008. *Eve Online Terms of Service.* Reykjavík: CCP. Available at http://community.eveonline.com/support/policies/eve-tos/ (updated link, 2013)
CCP. 2012a. Eve Online End User License Agreement. Available at http://community.eveonline.com/support/policies/eve-eula/
CCP. 2012b. Team Security – Now with 100% more Anti-RMT. Available at: http://community.eveonline.com/news/dev-blogs/28581
CipSoft. 1997. *Tibia*. Regensburg: CipSoft. Available at http://www.tibia.com
CipSoft. 2009a. *Privacy Policy.* Available at http://www.tibia.com/support/?subtopic=legaldocuments&page=privacy
CipSoft. 2009b. News Ticker. Available at: http://www.tibia.com/news/?subtopic=newsarchive&id=940&fbegind=1&fbeginm=12&fbeginy=2008&fendd=5&fendm=5&fendy=2009&flist=11111111
CipSoft. 2010a. Anti-Cheating Measures Reloaded. Available at: http://www.tibia.com/news/?subtopic=newsarchive&id=1207&fbegind=21&fbeginm=1&fbeginy=2010&fendd=21&fendm=1&fendy=2010&flist=11111111
CipSoft. 2010b. Open Letter to Game Masters. Available at http://www.tibia.com/news/?subtopic=newsarchive&id=1417
Coleman, Sarah and Nick Dyer-Witheford. 2007. Playing on the Digital Commons: Collectivities, Capital and Contestation in Videogame Culture. *Media, Culture & Society* 29 (6): 934-953.
Consalvo, Mia. 2007. *Cheating: Gaining Advantage in Videogames*. Cambridge, MA: MIT Press.
Council of Europe. 2008. Human Rights Guidelines for Online Games Providers. Available at http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf%282008%29008_en.pdf
Curran, James, Natalie Fenton and Des Freedman. 2012. *Misunderstanding the Internet.* Oxon: Routledge.
Dean, Michael. 1999. *Governmentality: Power and Rule in Modern Society*. London: Sage.
Deleuze, Gilles and Felix Guattari. 1987. *A Thousand Plateaus*. London: Athlone.
De Paoli, Stefano, Maurizio Teli and Vincenzo D'Andrea. 2008. Free and Open Source Licenses in Community Life: Two Empirical Cases. *First Monday* 13 (10). doi:10.5210/fm.v13i10.2064
De Paoli, Stefano and Aphra Kerr. 2010. The Assemblage of Cheating: How to Study Cheating as Imbroglio in MMORPGs. *The Fibreculture Journal* 16. Available at: http://sixteen.fibreculturejournal.org/the-assemblage-of-cheating-how-to-study-cheating-as-imbroglio-in-mmorpgs/
De Paoli, Stefano and Aphra Kerr. 2012. On Crimes and Punishments in Virtual Worlds: Bots, the Failure of Punishment and Players as Moral Entrepreneurs. *Ethics and Information Technology*14(2): 73-87.
De Landa, Manuel. 2001. *Panspectron.* Available at http://www.firstpulseprojects.com/panspectron.html
De Prato, Giuditta, ClaudioFeijóo, Daniel Nepelski, Marc Bogdanowicz, and Jean-Paul Simon. 2010. Born Digital/Grown Digital. Assessing the Future Competitiveness of the EU Videogame Software Industry. Seville JRC - IPTS. Available at: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=3759
de Zwart, Melissa. 2009. Piracy vs. Control: Models of Virtual World Governance and Their Impact on Player and User Experience. *Journal of Virtual Worlds Research: Technology, Economy, and Standards* 2 (3). doi:10.4101/jvwr.v2i3.663.
Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison.* Second edition. (English Translation.) London: Vintage.
Fuchs, Christian 2011. New Media, Web 2.0 and Surveillance. *Sociology Compass* 5(2):134-147.
Gandy, Oscar H., Jr. 2012. Matrix Multiplication and the Digital Divide. In: *Race after the Internet*, eds Lisa Nakamura and Peter Chow-White, 128-145. New York: Routledge.
Genette, Gérald. 1987/1997. *Paratexts. Thresholds of Interpretation*. Cambridge: Cambridge University Press.
Gillespie, Tarleton. 2010. The Politics of Platforms. *New Media & Society* 12 (3): 347-364.
Gillespie, Tarleton. 2014. The Relevance of Algorithms. In: *Media Technologies*, eds Tarleton Gillespie, Pablo J. Boczkowski and Kirsten Foot, 169- 194. Cambridge, MA: MIT Press.
Gray, Jonathan. 2010. *Show Sold Separately. Promos, Spoilers, and Other Media Paratexts*. New York: New York University Press.
GuildStats. 2014. Chair Fighter Refugia – Insomniac Entries. Available at http://www.guildstats.eu/character?nick=Chair%20Fighter%20Refugia
Haggerty, Kevin D. and Richard V. Ericson. 2000. The Surveillant Assemblage. *The British Journal of Sociology* 51 (4):605-622.
Humphreys, Sal. 2008. Ruling the Virtual World. Governance in Massively Multiplayer Online Games. *European Journal of Cultural Studies* 11 (2):149-171.
Humphreys, Sal. 2009. Discursive Constructions of MMOGs and Some Implications for Policy and Regulation. *Media International Australia* (130):53-65.
Introna, Lucas D. and David Wood. 2004. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society* 2(2/3): 177-98.
ISFE. 2010. "European Commission Communication on a Comprehensive Approach to Personal Data Protection." In: the *European Union ISFE Statement*. Brussels: Interactive Software Federation of Europe.

http://www.isfe.eu/sites/isfe.eu/files/attachments/icdp_high_level_statement_on_data_protection.pdf (accessed May 2013).
ISFE. 2012. ISFE Position on the proposed Data Protection Regulation. Brussels: Interactive Federation of Europe. http://www.isfe.eu/sites/isfe.eu/files/attachments/isfe_position_on_the_data_protection_regulation_proposals_december_2012.pdf Accessed May 2013
Juul, Jesper. 2002. The Open and the Closed: Games of Emergence and Games of Progression. In: *Computer Games and Digital Cultures*, ed. Frans Mäyrä, 323-329. Tampere, Finland: Tampere University Press.
Karppi, Tero and Olli Sotamaa. 2012. Rethinking Playing Research DJ HERO and Methodological Observations in the Mix. *Simulation & Gami*ng 43(3): 413-429.
Keatinge, Max. 2010. *The Expression and Constraint of Human Agency Within the Massively Multiplayer Online Games of World of Warcraft and Eve-Online: A Comparative Case Study*, MLitt thesis, Sociology, National University of Ireland Maynooth, Ireland. http://eprints.nuim.ie/2249/
Kerr, Aphra. 2006. *The Business and Culture of Digital Games: Gamework/Gameplay*. London: Sage.
Kimppa, Kai, and Bissett, Andrew. 2005. The Ethical Significance of Cheating in Online Computer Games. *International Review of Information Ethics* 4: 31–38.
Koster, Raph. 2000. Declaring the Rights of Players. Available at http://www.raphkoster.com/gaming/playerrights.shtml
Kücklich, Julian. 2009. Virtual Worlds and Their Discontents: Precarious Sovereignty, Governmentality, and the Ideology of Play. *Games and Culture* 4 (4): 340-352.
Lastowska, Greg. 2010. *Virtual Justice: The New Laws of Online Worlds.* New Haven, CT: Yale University Press.
Lessig, Lawrence. 1996. *Code V2*. New York: Basic Books.
Lyon, David. 2006. *Theorizing Surveillance: The Panopticon and Beyond.* Portland: Willan Publishing.
Lunenfeld, Peter. 2000. *The Digital Dialectic: New Essays on New Media*. Cambridge, MA: MIT Press.
MacCallum-Stewart, Esther. 2011. Conflict, Thought Communities and Textual Appropriation in MMORPGs. In: *Online Gaming in Context. Routledge Advances in Sociology*, eds Garry Crawford, Victoria Gosling and Ben Light, 40-59. London: Routledge.
Malaby, Thomas M. 2007. Beyond Play: A New Approach to Games. *Games and Culture* 2 (2):95-113.
Marx, Gary. 2007. What's New about the 'New Surveillance'? Classifying for change and Continuity. In: *The Surveillance Studies Reader*, eds Sean Hier and Joshua Greenberg, 83-94. Maidenhead: Open University Press.
Nieborg, David and Shenja van der Graaf. 2008. The Mod Industries? The Industrial Logic of Non-Market Game Production. *European Journal of Cultural Studies* 11 (2):177-195.
Oudshoorn, Nelly and Trevor Pinch. 2008. User-Technology Relationships: Some Recent Developments. In: *The Handbook of Science and Technology Studies*, edited by Edward J. Hackett, Olga Amsterdamska, Michael Lynch and Judy Wajcman, 541-565. Cambridge, MA: MIT Press.
Pskonejott. 2006-2009. Homepage of Pskonejott. Available at http://www.pskonejott.com/otc_info.php
Puppis, Manuel. 2010. Media Governance: A New Concept for the Analysis of Media Policy and Regulation. *Communication, Culture and Critique* 3 (2):134-149.
Silverman, Mark and Bart Simon. 2009. Discipline and Dragon Kill Points in the Online Power Game. *Games and Culture* 4 (4): 353-378.
Simon, Bart. 2005. The Return of Panopticism: Supervision, Subjection and the New Surveillance. *Surveillance & Society* 3 (1): 1-20.
Taylor, T. L. 2006a. *Play Between Worlds: Exploring Online Game Culture.* Cambridge, MA: MIT Press.
Taylor, T.L. 2006b. Beyond Management: Considering Participatory Design and Governance in Player Culture. *First Monday* 11 (7). doi:10.5210/fm.v0i0.1611
Taylor, T. L. 2006c. Does WoW change everything? How a PvP server, multinational player base, and surveillance mod scene caused me pause. *Games and Culture* 1 (4): 318–337.
Taylor, T. L. 2009. The Assemblage of Play. *Games and Culture* 4(4): 331-339.
Tschang, F. Ted and Jordi Comas. 2010. Developing Virtual Worlds: The Interplay of Design, Communities and Rationality. *First Monday* 15(5).doi:10.5210/fm.v15i5.2957
van Dijk, Jan. 2006. *The Network Society. Social Aspects of New Media*. Second ed. London: Sage.
Williams, Dmitri, Nicolas Ducheneaut, Li Xiong, Yuanyuan Zhang, Nick Yee and Eric Nickell. 2006. From Tree House to Barracks: The Social Life of Guilds in World of Warcraft. *Games and Culture* 1 (4): 338-361.
Whitson, Jennifer. 2010. Rule Making and Rule Breaking: Game Development and the Governance of Emergent Behaviour. *Fibreculture* (16). Available at: http://sixteen.fibreculturejournal.org/rule-making-and-rule-breaking-game-development-and-the-governance-of-emergent-behaviour/
Yan, Jeff and Hyun-Jin Choi. 2002. Security Issues in Online Games. *The Electronic Library* 20(2): 125-133.
Yan, Jeff, and Brian Randell. 2005. A Systematic Classification of Cheating in Online Games. In: *Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support for Games,* 1-9. Hawthorne, NY: ACM Press.
Zabban, Vinciane. 2011. What Keeps Designers and Players Apart? Thinking How an Online Game World is Shared. In: *Think Design Play.* Utrecht: DiGRA/Utrecht School of the Arts. http://www.digra.org/digital-library/publications/what-keeps-designers-and-players-apart-thinking-how-an-online-game-world-is-shared/
Zackariasson, Peter and Timothy L. Wilson. 2012. *The Video Game Industry. Past, Present Formation and Future*. New York: Routledge.