Social Games: Privacy and Security

Mathias Fuchs

Social Games: Privacy and Security

Mathias Fuchs

The University of Salford, School of Art & Design, Manchester, United Kingdom
mathias.fuchs@creativegames.org.uk

Abstract. Recent online gaming developments and para-gaming environments, i.e., the social software tools to communicate with fellow gamers, report, discuss and disseminate assets and experience, strongly resemble social media like Facebook or Twitter. It has therefore been suggested that games like World of Warcraft, Little Big Planet, The Godfather, or The Secret World should be called "social games." Privacy and security is an issue in these social games, as the players of these games do often not realize that they inhabit environments that have real estate outside the safe borders of the Magic Circle. The games companies harvest information about the players in ways that are far from transparent. The author will present examples of data mining and harvesting of data within a playful environment, analyze code segments that implement data collection, and suggest methods of refusal, sabotage, or disclosure of breeches of contract.

Keywords: social games, magic circle, scripting languages, digital footprint, computer forensics

1 Digital Surveillance

Surveillance has been associated with punishment, with the notion of crime, and with torture or imprisonment. It has been described as adding to a disciplinary technique that penetrated modern society and became apparent in the structure of prisons, hospitals, schools and military organizations [1], [2]. Authors like Michel Foucault have focused on the institutional backbone of the modern national states to describe how discipline emerged as a new technological power [1]. In his analysis leisure, entertainment or games play hardly more than a minor role. It seems that the "*Magic Circle"* that used to have ring-fenced play from all of society's evil [3], has also kept surveillance out. There is of course and has always been cheating, hiding and penalties in games, but those were not considered criminal acts, camouflage or punishment in a Foucauldian sense. Recent developments in games technology, but also the social changes that stem from the phenomenal success of computer games challenge the concept of the magic circle [4], [5] and ask for an answer to the question of whether gaming can be seen as ordinary social practice that is influenced by power structure, economic system, mediatic transformations, and real world relevance in general [6].

It has been suggested that computer games that build upon a large number of online players and in particular games that are embedded in a framework of para-ludic

activities like chats, memorabilia exchange, fanzines, gadget shops, and the like should be called "social games." Such are World of Warcraft, Little Big Planet, Unreal Tournament, The Godfather, or The Secret World.

Privacy and security is an issue in these social games, as the players of these games often do not realize that they inhabit environments that have real estate outside the safe borders of the Magic Circle. The games companies harvest information about the players in ways that are far from transparent. Data harvesting tools and technologies include the following: path tracking, eye tracking, heat maps, activity monitoring, non-game user information retrieval, and digital forensics.

Data visualization toolkits like the one offered by *Epic Megagames* and less well-documented surveillanceware allows for the recording of location, time and speed of movement, appearance and dress code, aggressiveness, solidarity, social behaviour, anti-social behaviour, and many other session attributes.

2 Social Games Data Harvesting Technology

When playing online games the players leave traces on the terrain they wander about that are more accurate than footprints in the snow and certainly much longer lasting. It is of importance to game developers to track down where players used to walk. It is also important for game developers to know which possible paths are highly frequented and which ones are rarely used. Almost every modern game engine has built-in functions to record, store and transfer these paths to the central server, that have been taken by a player at a given time. Many game engines also offer tools to analyse huge sets of paths and to visualize the statistical data generated from these data sets. Alastair Hebson's *Unreal Visualisation Toolkit* (UVT) allows users to record the paths that players make on a given *Unreal* map. The programmer's company that aptly calls themselves *Digital Footprints* offers a data log mutator and a screen capture mutator. Mutators are add-ons to the game engine that perform special operations enhancing standard gameplay. If the implementation of the mutator is not transparent to the user and if the programmer does not announce those special operations, no gamer would suspect that anything unusual takes place during gameplay. Whilst this is not a problem when used by games developers to create more interesting games, to optimize gameplay balance or to design terrain of high unpredictability, it poses a problem when used by parties with other interests. A marketing and advertising company can read whether in-game ads have been visited, it can observe whether certain content has been approached or what the mobility patterns of the players are. Players can therefore easily be classified as following certain consumer patterns, mobility modes or types of behaviour. The observation becomes even more useful when in-game eye tracking technology is used. Eye tracking is not at all easy in physical situations, but when the virtual eye is tracked in a computer game the accuracy of measurement is at a maximum. The data log mutator can record how long a player has been looking at an in-game ad, how often and how long he or she was focusing on an object or a detail belonging to that object. Games become a digital panopticon that outperform Bentham's invention: The ones that are under surveillance are not only deprived of facing their wardens, they do not even know that the wardens are looking at them.

Surveillance algorithms become more powerful when they collect not only individual user data, but create complex statistical data. The location of an individual user is not of high interest for market analysis, a heatmap generated from the locations where millions of users walk through is of great interest. A heatmap can as a 2D graphical representation indicate behavioural patterns, preferences, gaps in the attention or knowledge of the user.

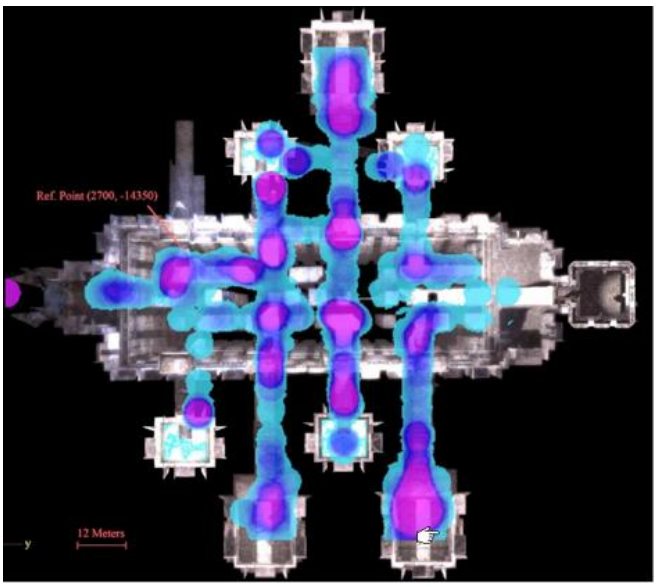

Fig. 1. Automatically generated heatmap of a Unity3D level. Frequently accessed areas are colour-coded in purple, rarely visited areas are in light blue.

At first sight one might think that the purpose of this is to track user experience throughout the world in order to assess which areas the gamers find interesting and which areas they are avoiding. This is often said to be used for debugging purposes or to improve gameplay for future updates. *Epic Megagames* states: "The purpose of this is to track user experience throughout the world in order to assess which areas the gamers find interesting and which areas they are avoiding" [7]. It is however quite obvious that the same map could easily be enhanced with information that goes beyond in-game information and contains user information or private data.

Code example. 1: Code sequence for the Unity3D player class to store player positions and to add personal user data to the generated log file that is contained in the file devlist.txt

```
var positionTrackingFrequency : int = 2; //How often to
store player position
private var timer : float = 0;           //The timer
```

```
static var posArray : Vector2[]; //Local array storing
player position
private var arrayIterator : int = -1;

function Update(){
    timer += 1 * Time.deltaTime;
      if(timer >= positionTrackingFrequency){
         storePos()}}

function storePos(){
    timer = 0;
    var localArray : Array = new Array();
    if(posArray != null)
        localArray = new Array(posArray);
    localArray.Push(Vector2(transform.position.x,
transform.position.z) )
    posArray = localArray.ToBuiltin(Vector2);
    arrayIterator++;
    Debug.Log(" " + posArray[arrayIterator] + "
Iteration =  " + arrayIterator);}

import System.IO;
var fileName = "devlist.txt";

function ReadPersonalData () {
    var sr = new StreamReader("C:" + "/" + fileName);
    var fileContents = sr.ReadToEnd();
    sr.Close();

    var lines = fileContents.Split("\n"[0]);
for (line in lines) {
    Debug.Log (line);}}
```

The information saved by the function storePos() saves the player's position at a certain interval, and the function ReadPersonalData() in the code example above contains information about the graphics card, processor, WiFi equipment and other devices that are installed on the player's PC, in the case of the author's PC a total of 168 devices. It is beyond the knowledge of most Unity users that such detailed information is polled and can easily be transferred to a company server via TCP/IP protocol. In this regard the algorithms providing the surveillance possibilities implement what Foucault called an "unequal gaze" [1], the constant possibility of observation, a one-directional view of the observer upon the information the user holds.

It does not happen very often that gamers become aware of path tracking, eye tracking or other surveillance techniques, and even less often do users complain about it. A recent protest about data harvesting in games took place, when German *Battlefield 3* players sued the company *Electronic Arts (EA)* to stop spying on data

that leaked to them whenever their game *Battlefield* was played. The online software component *Origin*, which was originally declared to spy on license fraud and to illegally install software from *EA,* seems to have the potential to send non-authorized user data to the company's server. The German television news programme "die Tagesschau" reported on the 8th of May 2012 that Thomas Schwenke, the lawyer of the plaintiffs in the Battlefield lawsuit, declared that "what looks like a copy protection mechanism, actually works like spyware" [8]. Evidence has been presented in this case that private data has been transferred to a server of *Amazon* company. As a partial success German gamers are now allowed to return copies of *Battlefield 3* to stores. The German retailers *Media Markt* and *Saturn* have given refunds to customers for used editions of Battlefield 3, even after their PC keys had been redeemed. But even so, *Electronic Arts* did not concede to having violated user rights. "We have updated the End User License Agreement of Origin, in the interests of our players to create more clarity. Origin is not spyware. Neither do we use nor install spyware on the PCs of users." The updated End User License now contains a line that states: "We have taken every precaution to protect the personal and anonymous user data collected." This seems to say that there is still user data being collected and that *Electronic Arts* keeps the right to do with it whatever they want. This is not a unique case; other companies operate in a similar way.

Linden Labs, for example, has stated: "Our Privacy Policy sets forth the conditions under which you provide personal and other information to us. You understand and agree that through your use of the Service you consent to the collection and use of your information in accordance with our Privacy Policy. If you object to your information being used in this way, please do not use the Service."

3 Digital Panopticon

If social games companies have the possibility of establishing a system of surveillance, and if they do so sometimes in individual cases, or even regularly on a large scale, then one could rightly ask how far the encompassing surveillance system within social games resembles Bentham's Panopticon - and in what respect it differs from the latter. There is no doubt that digital surveillance has a greater ability to surveil subjects than the brick-and-mortar structures Foucault was worried about. The computer game *Battlefield 3* that has recently been accused of spying on its users, sold 5 million copies in its first week of sales and, thereby, beat *Gears of War 3* and *FIFA 12*, each of which sold 3 million copies. Digital surveillance resembles the processes that lead to discipline in a Foucauldian sense [1], [2] by replacing arbitrary actions of those who hold power with a systematic and anonymous system of surveillance. Foucault points out that the opacity of the system of surveillance contributes considerably to its success. In digital online environments an end-user agreement usually empowers the provider of the environment to investigate secretly, to pronounce judgment without the right of appeal, and to punish users by banning them from their online environment.

In *Linden Lab's Second Life* the end-user agreement demands that [9]:

" …you agree that you shall not:

(i) take any action or upload, post, e-mail or otherwise transmit Content that infringes or violates any third party rights;

(ii) impersonate any person or entity without their consent, including, but not limited to, a Linden Lab employee, or falsely state or otherwise misrepresent your affiliation with a person or entity;

(iii) take any action or upload content that is harmful, threatening, abusive, harassing, causes tort, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable."

In case of an infringement of these conditions, users will, without having seen any evidence of the criminal procedure, be banned from *Second Life*. That any action of the criminal that is "otherwise objectionable" can lead to punishment evokes in a cynical manner what prisoners in the Gulag or in torture camps like camp Guantanamo experience. Foucault's description of discipline and the procedure of investigation fits well with the procedures *Linden Lab* executes, when banning inhabitants. These procedures do not relate to transparent codes of law, but to the symbolic affirmation of sovereign power. This sovereign power once was the king, the army, the national state, and is nowadays *Linden Lab*, *Electronic Arts* or *SONY*. These new sovereign powers can even override federal law or state law. As *Linden Lab* put it: "As a condition of access to the Service, you release Linden Lab (and its officers, directors, shareholders, agents, subsidiaries, and employees) from claims, demands, losses, liabilities and damages (actual and consequential) of every kind and nature, known and unknown (…) If you are a California resident, you waive California Civil Code Section 1542, which says: 'general release does not extend to claims which the creditor does not know or suspect to exist in his favor at the time of executing the release, which if known by him must have materially affected his settlement with the debtor.' If you are a resident of another jurisdiction, you waive any comparable statute or doctrine" [9].

There are similarities of the digital Panopticon, but there are also differences. For Foucault it was the body that worked as the physical centre and constituting factor for discipline and punishment. In the digital realm bodies are replaced by locations of actors. IP addresses or GPS-coordinates replace what the physical body once has been for surveillance. That is why Metadata is so important for a system of control. Once every image is time-stamped and location-stamped, the process of monitoring the generation and dissemination of information can be optimized. Software can be identified as legally copied or illegally cloned; emails can be assigned to paths; mail servers and client IDs images can be tracked down for the real physical location at which they were taken. The system of micro-power has no longer to refer to the body of the individual, but to the location of the actors in the system. In the age of disembodiment "disciplinary power" is no longer – as Foucault had it – coinciding with the birth of "an art of the human body," but with the emergence and success of location-based media and the importance of the politics of space. Indeed, when Foucault spoke of the four characteristics of individuality that discipline constructs as cellular, organic, genetic, and combinatory, I would suggest that digital discipline replaces the organic with the location-based whereas cellular, genetic and combinatory characteristics remain essential for digital discipline. Cellular aspects guarantee that the identity of the units is not corrupted by clones, copies or replicated assets. Genetic consistency is essential for tracking down generations of code,

programme versions and the whole process of inheritance in object-oriented systems. Finally the combinatory serves to enhance the power of individual actors, to form clouds and distributed computing, and to establish discipline not only in the individual units, but in large systems as well.

4 Counter-Strike

Is there a chance to escape digital surveillance, if it is as powerful as the technical system suggests? Three suggestions should sketch alternative routes to escaping, playing with, and fighting digital surveillance.

4.1 Camouflage

This is probably the least delightful alternative, but still a chance to escape surveillance. The possibility of setting up firewalls, playing games secretly and in solitude without using the multiplayer mode clearly exists. One might choose to not connect to the Internet, and send emails anonymously from hotmail accounts at Internet cafes, but what life is that? Remaining completely invisible will turn the social gaming experience into a digital hermitage.

4.2 Manipulation of Data

Users with programming skills and with a profound knowledge of the systems they use can write software that filters the information they provide to the outside world or they can alter information that social games transmit to the game companies and the providers. The functions in programme example.1 would only require minor amendments to avoid the leak that prepares the device information for transmission. Change

```
var fileName = "devlist.txt";
```

into

```
var fileName = "noinformation.txt";
```

Then put a text file on your C: drive that contains any message to the games company and it will be sent there. This process of course, is very time consuming and one would enter a rat race of finding out where the next data leaks are in the programmes one has bought can be found.

4.3 Cloning and Multiple Identities

There have been successful attempts to escape control mechanisms by disclosing or confusing the personalization of actors in social games. In *Second Life,* there have been protests that gathered identical clones of avatars to show up at places and to demonstrate against constraints of *Second Life* civilian rights. By sharing an identical

appearance, such interventions make a strong statement against the pseudo-individualism that is promoted by the company. The creation of self-spawning clones is subverting the possibilities of tracking down individuals and punishing them for breeches of the End User License Agreement. “Every Resident has a right to live their Second Life. Disrupting scheduled events, … following or self-spawning items” are forbidden in Second Life as are demonstrations in real life authoritarian regimes. And in the digital world as well as in modern national states it is up to the sovereign, of course, to decide what a “disrupting event” is.

5 Conclusion

Social Games provide possibilities for monitoring user behaviour that other electronic media lack. In such games, it is not only possible to count how often a user visits a place where an advert is located; such games can also measure and document the duration of the eye contact with the object in question, to describe watching patterns (or listening patterns) in detail, and to relate this to game states, movement patterns, private information and any other conceivable information that can be retrieved from the gamer’s computer. The surveillance mechanisms that have been proven to have been installed in modern social games resemble the “unequal gaze” that Michel Foucault found characteristic for the technology of discipline and for the setting of Bentham’s Panopticon. There are, however, differences in the way modern surveillance works and how digital surveillance in social games works. The body as the centre of modern pre-digital surveillance has been replace by location as the main instrument of surveillance and a new micro-politics of power emerges that causes new threads but also new hopes for resistance.

References

1. Foucault, M.: Discipline and Punish. Vintage Books (1995, orig. in French 1975)
2. Foucault, M.: Birth of the Clinic. Vintage Books (1973, orig. in French 1963)
3. Huizinga, J.: Homo ludens. Vom Ursprung der Kultur im Spiel. Reinbek bei Hamburg (1987, orig. in Dutch 1938)
4. Liebe, M.: There is no Magic Circle. On the Difference between Computer Games and Traditional Games. In: Günzel, Stephan, Mersch, Dieter (eds.) Conference Proceedings of The Philosophy of Computer Games 2008, Potsdam, pp. 324-341(2008)
5. Günzel, S.: Der reine Raum des Spiels – Zur Kritik des Magic Circle. In: Fuchs, M., Strouhal, E. (eds.) Passagen der Spiele II, pp. 189-202. Springer, Vienna, New York (2010)
6. Montola, M.: Exploring the Edge of the Magic Circle. Defining Pervasive Games. In Proceedings of the 6th DAC Conference. Copenhagen: IT University of Copenhagen (2005)
7. Unreal Developer Network webpages, by Epic Games, http://udn.epicgames.com/Three/GameStatsVisualizerReference.html
8. German ARD Broadcasting Network reports on its webpages on 8th May 2012, http://www.tagesschau.de/inland/battlefield100.html
9. Second Life EULA, http://secondlife.com/corporate/tos.php