DIO: A Surveillance Camera Mapping Game for Mobile Devices

Rafael de Almeida Evangelista
Cidade Universitária Zeferino Vaz Campinas (BR)

Tiago C. Soares
USP – Universidade de São Paulo (BR)

Sarah Costa Schmidt
Cidade Universitária Zeferino Vaz Campinas (BR)

Felipe Lavignatti
Cidade Universitária Zeferino Vaz Campinas (BR)

Abstract: Surveillance cameras are fast-growing technologies in contemporary society. In poorer countries, they are used to curb urban crime; in richer nations, they are also employed to fight terrorist threats. In this scenario DIO arises, a mobile phone game (still in development) that deals with the rampant increase of surveillance cameras in urban spaces. The game promotes a collaborative mapping of cities by inviting players to complete the following tasks: 1) geolocate, photograph, and log surveillance cameras scattered around the city; 2) compete against the opposing team for control of the cameras. Once registered, those cameras become playable geolocation points with which players can interact when physically close. This article presents the basic game plot, rules, and dynamics as well as a discussion on the increasing financialization and marketization of personal data and how to approach these issues through gaming.

Submitted: October 17, 2016 – November 15, 2017

Keywords: surveillance; personal data; CCTV; pervasive games; GPS.

Corresponding author: Rafael de Almeida Evangelista, Labjor – Unicamp Rua Seis de Agosto, 50 - 3o piso, Cidade Universitária Zeferino Vaz Campinas – São Paulo, Brazil CEP 13083-873. Email: rae@unicamp.br

1. Introduction

Surveillance cameras are fast growing technologies in contemporary society. In Britain alone, one of the pioneering countries in installing public surveillance systems dependent on remote images, an estimated 5.9 million cameras are in use by public and private organizations (Barret 2013).

Security concerns are the main reason for the widespread use of surveillance cameras in cities – in poorer areas, to curb urban crime (Kanashiro 2008; Carr 2016); in richer areas, to fight terrorism threats (as illustrated by the large number of devices installed in Manhattan by the New York Police Department). In NY, there are 4,000 CCTV cameras, public and private, operating in a single part of the city. In Boston, a similar, albeit smaller system was employed to identify the perpetrators of the 2013 terrorist attacks (Kelly 2013). Writing on the use of CCTV in Barcelona, Clavell (2011, 525) states that it became popular as "part of a broader project to promote 'civility' and eliminate 'anti-social behaviour'". Working properly or not, CCTV has become part of our cultural repertoire (Groombridge 2002).

Surveillance cameras are one of many technologies – like traffic sensors, pollution monitors, flood sensors and others – that are becoming part of the infrastructure of "smart cities". These initiatives use data-collection and analytics in support of city planning, infrastructure maintenance, preemptive policing, and management of urban flows and mobilities. Leszczynski (2016) cites centralized command-and-control facilities (that heavily depend on CCTV to function) as one of the examples of real-time urban big data for managing the here-and-now. Besides that, those data-driven contemporary technologies work as a safeguard against social and natural disasters, "subscribing the horizon of possibilities to exclude potential scenarios deemed undesirable or deleterious" (Leszczynski 2016, 1692).

Concerns over vigilantism and the real effectiveness of CCTVs in fighting violence make their use somewhat controversial. In many democratic nations, civil rights organizations have criticized the proliferation of surveillance systems, claiming privacy rights violations. The ACLU (American Civil Liberties Union), for example, argues that cameras 1) would be susceptible to abuse; 2) are not proven to be effective; 3) would not be properly controlled; and 4) would have a chilling effect on public life (ACLU).

In Latin America, the legal frameworks concerning surveillance are fragile and lack specific regulation (Firmino et al. 2013). In countries like Brazil, home to global events like the 2014 FIFA World Cup and the 2016 Olympics, the government, in an effort to prevent terrorism, has expanded the reach of surveillance operations. Kitchin (2014) understands that effort as related to the current practice of governments using real-time analytics to manage aspects of how a city functions and is regulated. He mentions the Centro de Operações da Prefeitura do Rio (COR) as an example of an attempt to draw all kinds of surveillance and analytics into a single hub:

(...) the Centro De Operacoes Prefeitura Do Rio in Rio de Janeiro, Brazil, a partnership between the city government and IBM, have created a citywide instrumented system that draws together data streams from thirty agencies, including

traffic and public transport, municipal and utility services, emergency services, weather feeds, and information sent in by employees and the public via phone, internet and radio, into a single data analytics centre (...). Here, algorithms and a team of analysts process, visualize, analyze and monitor a vast amount of live service data, alongside data aggregated over time and huge volumes of administration data that are released on a more periodic basis, often mashing the datasets together to investigate particular aspects of city life and change over time, and to build predictive models (...). This is complemented by a virtual operations platform that enables city officials to log-in from the field to access real-time information. (Kitchin 2014, 6)

Sadowski and Pasquale (2015) cite COR as the best example of a *smart shock*, "wherein a city undergoes a quick, large-scale integration of 'smart' ideals, technologies, and policies into an existing landscape". According to them, the city of Rio was turned into a system for optimization and securitization, with the amplification of already existing practices of militaristic urban control.

An article from the technology magazine "Motherboard" (Kayyali 2016) reports that the process started just before the 2014 World Cup, spawning "drones, facial recognition goggles that can scan 400 faces a second and check them against a database of up to 13 million images, and 122 surveillance helicopters, many outfitted with HD surveillance and infrared cameras". This technology has also been used to stifle political protests, like the demonstrations that questioned the extent of investment in the 2014 World Cup and in the 2016 Olympics in Rio de Janeiro. An extensive news report from the news agency "Pública" shows how the surveillance equipment bought for those major international events was expected to be used both against possible terror acts and for fighting urban violence, and how political protests were treated as a major threat to the security of tourists and athletes (Viana et al. 2017).

However, most cameras spread throughout Brazil perform ordinary functions – they are not solely in the hands of the state for crime prevention, gathering evidence, or legal proceedings. Normally, violence prevention is jumbled in with practices of segregation and social cleansing (Kanashiro 2008). Cheaper technology and the popularization of surveillance equipment have made it nearly impossible to commute in urban areas without being filmed. New digital image processing technologies enable widespread identification procedures, and its uncontrolled use interfere with the management of public areas: police departments are increasingly engaging in preemptive operations, leading to abuse, racial profiling, and gentrification[1].

[1] Vlahos (2012) inform us about the use of "data-rich computer technology" being used by several police stations across the US to predict crimes. Jouvenal (2016) reports on Real Time Crime Centers functioning in US cities like Fresno and Seattle, in which individuals can be scored based on their threat level. After helping the Seattle Police Department to launch its Real Time Crime Center, the

Cameras are being used to watch employees and customers in shopping malls, bars, and stores for a number of reasons. In public spaces, they also monitor areas such as streets and sidewalks, mapping – and, in some cases, preventing – the circulation of determined groups. In both cases, these groups cannot do anything to prevent their identification and monitoring. And public squares, where pedestrians are of particular interest to the real estate business, are monitored to exclude 'undesirable' groups (Kanashiro 2008; Kanashiro 2006). Put together, such space monitoring hardware and software lead to an *automatic* production of space (Thrift and French 2002), with relevant social consequences. As something written by humans, software (and hardware) challenges us to comprehend these new forms of technopolitics and practices of political invention: "politics of standards, classifications, metrics, and readings" (Thrift and French 2002, 331). The software and hardware designed to perform functions on space also inherit the bias, preferences and opinions of those who made them. Leszczynski (2016) also points in that direction when she states that as the city is subsumed within the data-security assemblage, algorithmic governmentality follows the urban realities of inequalities.

As said before, cameras targeting public areas such as squares, streets, and sidewalks, are used mostly for two purposes: to control urban violence and crime; and to manage traffic. In both cases, the installation and control of surveillance equipment is usually provided by private or public bodies; but there is a caveat – when it comes to the institutional management of surveillance systems, government authorities may also share the control with private, outsourced agencies (Cardoso 2012)[2]. In some situations, these roles and functions may be intertwined, such as when traffic control cameras record a significant event "by accident".

Gated communities, a housing modality that has grown tremendously in Brazil (currently accounting for nearly 2% of all households; Uchinaka 2011), boast security as one of its major desirable features – a promise epitomized by the large number of monitoring cameras usually found in them. In developing countries, the fear of urban violence is one of the main reasons for the growth of this type of housing, and some form of complementary "technical fix" (Firmino et al. 2013) is frequently installed to further secure the physical enclosure of the area. In common areas, such as elevators, lobbies, and leisure areas, cameras may give rise to abusive actions suffered by residents as well as employees.

---

private company Via Science was involved in the development of the predictive features of CrimeRadar, a publicly available crime-forecasting tool based on open-access that was launched in Rio de Janeiro after the Olympic Games of 2016 (Capps 2016).

[2] Cardoso (2012) tells us about the involvement of at least three different companies besides the State Department of Police in the management of Rio de Janeiro's Command and Control Center (CCC).

Images are now easily stored and maintained for indefinite periods of time in databases. They can be sent to be examined in remote places and easily copied and multiplied. They can also be analyzed by software capable of identifying characteristics invisible to the human eye. Graham and Wood (2003) point the social effects of digitized surveillance, stressing that the current social conditions are the privatization of public spaces and services, coupled with a notion of citizenship linked to consumerism. The authors note that "digital surveillance also provides a new range of management techniques to address the widening fear of crime and the entrenchment of entrepreneurial efforts to make (certain parts of) towns and city spaces more competitive in attracting investors and (selected) consumers" (Graham and Wood 2003, 234-235).

There is evidence that the same measures meant to promote human security can, potentially, also foster feelings of insecurity, vulnerability, and exposition (Esposti and Santiago-Gomez 2015). Surveillance technology companies advertise the economic benefits of the use of their equipment in workplace environments. For example, one company claims that "business managers can study customers' shopping habits by studying videos recorded by surveillance systems.[3]"

2. Visualizing Surveillance

The tension between power, security, and freedom echoed in the cybercultural debate is longstanding. In the 1960s, in opposition to the institutions of technocratic control and censorship of the Cold War, social movements manifested deep concerns for freedom of expression and individual autonomy. In the United States, these movements would go on to stimulate communities that promoted social, artistic, and technological experiments, culminating in the microcomputer revolution and new cultural arrangements (Turner 2006). Influenced by the Free Speech Movement at the University of California, Berkeley in the 1960s, on through to the hobbyist computer clubs and experimental, autonomous communities scattered throughout California in the 1970 and 80s, Silicon Valley emerged as the epicenter of what would become a new, hegemonic knowledge management model. Through the idea of technological appropriation, the Cold War mainframe was reinvented into the microcomputer – and, as so, became part of a new, individual, cognitive apparatus. From desktops to laptops, and finally to smartphones and the internet of things, the computer became a device of higher technology, uniquely integrated to each individual user.

Castells (1996) claims that the prominence of the Californian techno-

[3] See https://reolink.com/why-does-your-business-need-video-surveillance (retrieved June 28, 2016)

scientific complex is embedded in a wider, international economic transformation. The delocalization of factories and production, and the emergence of financialization as the core of the western economy, created the need of an ever-stronger, ever-increasing machinery for the widespread data-management demanded by a global connected economy. Critics like Winner (1997), Barbrook and Cameron (1996), and Morozov (2014) expand on the worldview summarized by Castells, and counter the notion of a supposed neutrality on the role played by technology – especially when it comes to political economy and structural changes. These authors will articulate a critique of Silicon Valley, viewing in its latent technodeterminism an essentially ideological project – the *Californian Ideology*.

This movement, with its nod to the experimental propositions of technologists influenced by radical theorists such as Jacques Ellul (1964), Herbert Marcuse (2013[1964]), and Ivan Illich (1973), draws, however, on a powerful internal antagonism. While increasingly sophisticated individual control of technological devices offers possibilities for invention and disruption of asymmetric power structures, the colossal volume of data generated by these same devices unearths new monitoring and controlling tools. In the realm of the State or in independent groups, networking tools such as IMSI catchers (low-cost interceptors used in cellular networks), mesh networks, and hardware/software toolkits for remote monitoring create a scenario that not only increases government control but also sets in motion actions of dispute and resistance by a number of civil society groups, promoting a game of perpetual power and counterpower.

Bruno (2014) reminds us of the overlap between surveillance culture (video surveillance and social networks on the Internet) and the "society of the spectacle", with links to surveillance, blatantness, and pleasure. Surveillance cameras mimic the image (sometimes sound) capturing technologies which are the base of the most popular entertainment products of the twentieth and the twenty-first century. To observe using them, and to be observed by tkhem, involves a certain discipline of body and attitude, and are also practices associated with entertainment and expression.

The same thing that can be said about the relation between play and management can be said about games and surveillance. Koskela and Mäkinen (2016) state that surveillance and games are intertwined and that "examining the game elements of surveillance facilitates a broader understanding of how this practice moves beyond power and discipline". They also try to use the idea of game as a tool to dissect surveillance, offering five different metaphors. In one of them, they argue that surveillance can also be understood as a labyrinth, saying people can playfully navigate through surveillance spaces, sometimes trying to avoid being monitored.

In the relationship between the one who watches and the one who is being watched, issues such as the visibility or invisibility of surveillance devices should be discussed. While people and their actions are disci-

plined by the presence of surveillance cameras, the lack of public debate on their use only promotes the unregulated proliferation of the technology, increasing the cases of abuse. To study and map cameras can be an effort of resistance to its power. In a city that becomes aware of itself, "sentient" (because it is loaded up with information and communications technology), Thrift (2014) says that new technical-artistic interventions are required if we are not to become simply servants of the security–entertainment complex. Brighenti (2009) comments on the interplay between artists questioning the surveillance society and the ideoscape of surveillance forming a collective imagery about what security, insecurity, and control are about. He also points out that different kinds of recent art works can be interpreted as an attempt to deal with visibility regimes shaped by specific asymmetries.

Bruno (2014) points out that the "beginning of the dissociation of the see-and-be-seen principle, associated with the principle of 'unverifiableness' of power," is crucial to the fulfillment of one of the purposes of the panoptic machine described by Foucault – the automatic functioning of power:

> If you can discern the eye spying on me, then I dominate the surveillance, and I spy on it also, learning its intermittence and faults, and I can study its regularities and rid myself of it. If the eye is hidden, it looks at me, even when it's not seeing me. (Miller 2000, 78 quoted in Bruno 2014, 60)

The question arises: given the widespread use of video surveillance technology in contemporary society, and the broad, global use of portable devices for personal network-computing, what can we develop to physically expose many of these surveillance apparatus and information processing equipment in order to recognize, as best as possible, not only their existence but also their potential? On the other hand, what can we do to denaturalize their presence in urban settings in order to create a discussion on how to socially discipline them? Currently, it is impossible to dissociate digital networks from these devices. Digital images and sounds roam the networks, forming the raw material of entertainment and media products. Algorithms analyze the digitized content to recognize patterns, which are then cross-referenced with other databases.

Our proposal is a mobile app[4] that we are calling DIO: a playable, collaborative platform for the mapping of surveillance cameras through augmented reality and the geomapping of urban areas. The game is designed to be played daily, so that the flow of players (carrying their mobile devices) in monitored areas could be continuously processed and

[4] The app is in development stage and has financial backing from the Ford Foundation as part of a larger project named "Rede Latino–Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (Lavits): interseções entre pesquisa, ação e tecnologia", which is developed by Lavits (www.lavits.org).

turned into playable data. We intend by this to expose and discuss the presence and use of cameras, emphasizing the centrality of urban flows in the functioning of surveillance systems.

In his review of many art or intervention projects dealing with surveillance, Brighenti (2009) cites iSee (2001-2005), a now defunct web-based application that maps the locations of surveillance cameras in urban environments. Our effort is similar, but to achieve a comparable goal we use playful elements, focusing on the dissemination of mobile phones. Studying location-based social networks as Foursquare, Saker and Evans (2016) coin the term "playeur" to try to describe an engaged actor that develops relationships with space and place through intentional playful activities. To achieve that the playeur, like the "phoneur" (Luke 2006), uses his or her smartphone to change how the urban space is traversed. In this sense, DIO is a mobile game that relies on the player experience to engage in a critical relationship with regimes of visibility.

In the development process, we opted for narrative elements and gameplay structures aligned with that of other games that make intensive use of surveillance tools and personal data processing – games like Pokemon Go (2016), Watch Dogs (2014) and Ingress (2012). The purpose is twofold: on the one hand, we may offer structures with which players are already familiar; on the other hand, we will be able to engage in a critical appropriation of these schemes not for surveillance[5] but for discussion – although as O'Donnell (2014) says, the use of surveillance in one form or another is inevitable. Ingress (2012), which is also a game that relies on the mobility of the players, is particularly a case we want to address. Using gamification mechanisms, the game nudges its players to catalog historical buildings, street art and tourist landmarks. At the same time that it promotes "datafication of one's mobile life in exchange for the gift of play" (Hulsey and Reeves 2014), it is one of the best examples of the connection between gamification and big data and algorithmic surveillance. DIO uses a very similar game dynamic to put the surveillance at the core of the game plot.

Following Thrift and French (2002) on the discussion of the "automatic production of space", Graham and Wood (2003) recall the opacity and ubiquity of these computer systems and their process as a whole, as it becomes difficult to identify how the shift to automatic, digital and algorithmic surveillance is linked to profound changes in the political economy of urban space management. By giving prominence to these systems of imagery and informational surveillance, we want to contribute towards bringing them to the fore.

More than just plotting an accurate map of the cameras, pointing out exactly how many and of which type they are, we propose that these devices are turned into elements of an online environment in which players can interact, while also revealing that these devices actually exist and have

[5] No data regarding the player's identity will be stored or commercially used.

effects beyond the locations where they are found. We also suggest renewed discussions on technological re-appropriation: in the twentieth century, criticism of bureaucratic control by the military-industrial technocracy brought up new technologies and their use in the reshaping of power structures. Today, in the interconnectivity between the digital environment of the game and the real world, we want to discuss surveillance cameras and put them into focus.

To articulate the proposed debate, we offer – as an element to guide player actions – a background story that contextualizes aspects of the use and production of technology in contemporary society, such as the surveillance society (Lyon 2001), technology ownership, and political and economic uses of personal data.

Van Brakel (2013) suggests the need for a more generous understanding of what "play with surveillance" means. Playing with surveillance, she says, "can have a transformative effect both on the person playing but also on social and cultural norms". But she also alerts us to the possible normalizing effects it could have on how people perceive and give meaning to surveillance. Although we are using surveillance as a theme for the game and suggesting its daily use, our goal is to produce the exact opposite to a normalizing effect. The objective is to create awareness of the surveilling processes, in an effort to stimulate democratic questioning. Thrift and French (2002), when discussing the automatic production of space, suggest that, in the house of the near future, the operating system of the computer that runs the house would be as important as the roof. The cameras that today surveil the major cities of the world are one of its most important sensors. We want to incorporate the surveillance apparatus of the cities as an element of the game. Hulsey and Reeves (2014) and Stenros et al. (2011) tell us that many augmented reality games (ARGs) often incorporate non-players into the gaming experience. The game DIO is an effort to produce ludic awareness about the location and the interconnectivity of the informational and surveillance systems that currently pervade our everyday lives.

3. Storytelling and Development

Based on the worldwide use of smartphone geolocation tools, the game proposes primarily what could be understood as a new "layer" of use. The geocoding platform developed for the game is based on solutions commonly applied in other tools found in mobile devices, so that the players' actions, when it comes to input, classification, navigation, and database processing, are, strictly speaking, similar to the usability found in apps for restaurants, relationships, or taxis. It is a narrative that encourages not only the discussion of surveillance in public areas, but also the uses and possibilities of technological tools whose presence has be-

come "natural" in daily life. It is interesting to remember that the transnational surveillance structures uncovered by Edward Snowden (Greenwald 2014) in the early 21st century are based, in no small part, on the monitoring of personal devices such as laptops and smartphones.

The development of the narrative, as well as the technical and functional structures of the game, underwent a series of conceptual workshops involving the project's team. Apart from attending communications symposiums, the project team had conversations with technical experts and specialists in technology and policy, as well as inquiries into the state of the art in digital and experimental games conducted by research groups in Brazil[6]. From a Brazilian (and, probably, South American) standpoint, a main challenge in video game research seems to be the development of permanent, sustainable projects and interdisciplinary teams. The convergence of different academic expertise and faculties into development projects is in many cases a result of specific, individual interests, rather than institutional frameworks. Funding and programs devoted to research on digital games are still somewhat rare, despite a growing interest among the academic community. Even though a considerable part of the existing research and development may seem incipient and/or rather inconsistent, there appears to be an ongoing increase in the quality of the projects, both in their methods as well as in their results. Mapping (and mastering) these pitfalls has probably been one of the main tests faced by our team.

To transition from a concept to a playable platform, the development team researched the narratives and gameplay featured in games of all types and generations, as well as aesthetic references in documentation and products associated with videogames and their role in popular culture. There were also studies on thematic and dynamic narratives in film and science fiction literature. Collected data was organized into conceptual streams for eventual implementation into the game development by the project's tech team.

The term "cyberpunk" was officially adopted in the workshops. The decision to use the term has historical context as well: cyberpunks are the heirs of the cultural propositions of the 1960s and 1970s that culminated in the reinvention of the computer as a counter-hegemonic, organizational tool. Movements that, in their critical discussion of politics and technology, engaged in lengthy experiments with science fiction as an outlet for not only literary speculation, but also as a platform for political, technical and organizational experimentation. As Lee Felsenstein (2013) explains in his memories, the countercultural experimentation that led to the "hobbyist culture" and the "garage microcomputer" was heavily influenced by the ideas, groups and networks built around the science fic-

[6] See the *Congresso Brasileiro de Informática na Educação e Conferência Latino-Americana de Objetos e Tecnologias de Aprendizagem* (2015) http://-www.br-ie.org/pub/index.php/teste/issue/view/135 (retrieved March 30, 2016).

tion scene[7] of the 60s and 70s (Rossman 1972).

The visual patterns that were created for DIO resemble the science fiction of the late 1970s and 1980s. You can find below a screenshot of one of the first screens of the game, right after a player logs in. The game is a web-based application, so it works both on desktop computers and mobile phones. The following screen was taken from a desktop computer browser. You can see a button on the left of the screen to add a new mapped camera, and a small window with some player information.

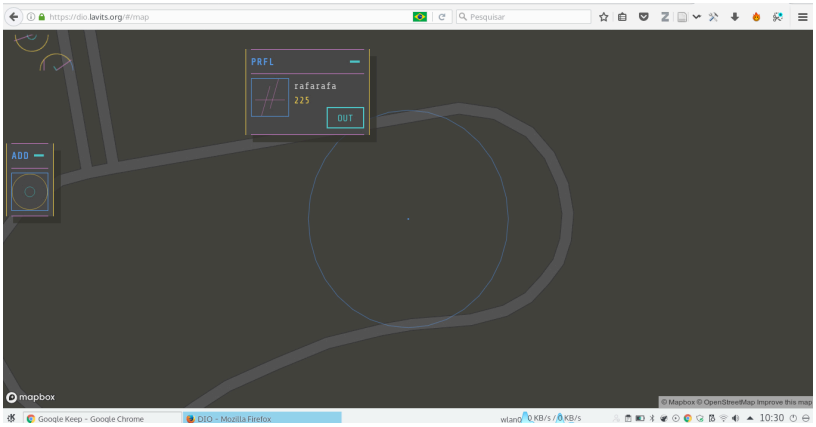

Figure 1 – Screenshot of the game from a desktop computer. The small blue dot represents the player's location. The blue line is the player's area of action.

4. Argument and Dynamics

The game seeks to trigger traditional role-playing gaming, unhinged and mediated by users and their collaborative groups. The development of the narrative and personal story of each player in the game plot is performed by managing the georeferencing platform and its data, without the use of guided navigational elements or 'closed off, on rails' playing levels. It is a Massively Multiplayer Online Game (MMOG) and also a pervasive game (also known as hybrid games, location-based games, and mobile games). Stenros et al. (2011) note that pervasive games are not played necessarily on computer screens (although they might use them)

[7] Ballard (1962), in the final decades of the twentieth century, summed up what came to be the New Wave of Science Fiction and its interface between counterculture and sci-fi: "The biggest developments of the immediate future will take place, not on the Moon or Mars, but on Earth, and it is inner space, not outer, that needs to be explored. The only truly alien planet is Earth".

or in predefined spaces or set times. Kerr et al. (2014) identified five elements that are part of the system of governance in MMOG (game code and rules; game policies; company community management practices; player participatory practices; and paratexts). They conceptualize these governance elements functioning as a "surveillant assemblage" (Haggerty and Ericson 2000). The assemblage Kerr et al. (2014, 333) typify and analyze "demonstrate that game governance by companies responds to, and shapes the behaviour of players but is often in flux, shifting and adjusting". One major challenge for the governance of DIO is to promote this flux according with the game goals.

At this phase of DIO's development we are focusing on the definition of the game's code and rules, as well as on its paratexts. The basic rules and game dynamics are mostly defined, although it should be modified according to feedback from gamers. Paratexts will be an important element to address the main social issues the game intends to thematize: the widespread deployment of surveillance cameras in urban areas; the growing digital management of urban spaces; and the economic use of personal data. Game policies should emphasize that DIO 1) is not a commercial project; 2) respects the privacy of its users by collecting only data essential for the game's proper functioning; and 3) is a free and open source project. The game should be freely available for iOS, Android and Windows phones, as it has been developed as a Progressive Web App (PWA). PWAs are regular web pages that can appear to the user like traditional applications, trying to combine features offered by browsers with the benefits of mobile experience.

Other elements should be dealt with before an alpha version is available. DIO is a game about a surveillant assemblage – the interconnection of CCTV, speed radars, computers, mobile phones etc. – which as an MMOG will require the use of other surveillant assemblages for its governance.

The proposed scenario is the 'very near future' – a reality in which artificial intelligence is used by governments as a tool for social control. To develop the story, we studied with special attention popular games such as Watchdogs, in which a supercomputer (a ctOS - Central Operating System) that connects everyone and everything – personal information, traffic lights, mobile phones, and security cameras – is implemented in Chicago, Illinois, after a hacker attack.

In our plot, governments and companies, to combat opposition, employ surveillance technologies that scan physical spaces and monitor digital networks. To improve this system, a multinational public-private partnership project is launched to create a technological standard. This protocol, developed with the objective of integrating public surveillance devices around the planet, is called Digital Information Operative (DIO). It is an effort to create an intelligent technical protocol that integrates cameras and forms a system in which all units are accessible remotely. Quietly test-launched, the project receives the collaboration of many companies

and technicians, who vindicate for globalized efforts for transparency and scorn upon alerts and claims of human rights violations. Shortly thereafter, the initiative is terminated, also quietly, and the project never officially goes into operation.

It would, however, all prove to be a farce. Once testing starts, the artificial intelligence that would integrate devices around the world becomes uncontrollable. With all cameras consolidated, it becomes impossible to cut them off from the network for a long period of time, being that DIO reestablishes lost connections. The project was discontinued and the autonomous existence of DIO was never publicly admitted for fear of negative backlash. And now, as a result, every camera in the world is subject to the control of DIO.

Every footage and image provided by the cameras is now online, available in a 'deep web' of sorts, and is accessed by political, economic, and technological operational groups. It is impossible to turn them off effectively. Governments and corporations can finally watch over and track everything. It is the end of privacy. DIO now fully displays and broadcasts society's weaker bodies, while members of power remain concealed and blanketed. Footage revealed in the network continues to be wielded by governments. After an effective disinformation campaign, the mere existence of DIO is seen as just a rumor, a ghost story.

For the overall public, DIO is just a conspiracy theory. However, for resistance groups, it is reality. Naturally, the resistance split into two distinct groups, with two different philosophies. The Blind group believes that the best action to take is to blind all cameras, because image capturing technology in itself is detrimental. The Lens group believes that the best way is to restore autonomy to the cameras, as well as to their original owners – if the devices are finally dissociated from DIO, their original owners (the companies) would make good use of them. Both groups apply these different outlooks not to fight against each other, but to battle DIO. Nevertheless, DIO ends up regenerating itself and reactivating and reincorporating the cameras to its network. The groups continue their fight in search of a permanent solution.

The game dynamics are inspired by controversial commercial games like Ingress and Pokemon Go. Hulsey and Reeves (2014) highlight that Ingress is an emerging form of digital economic exchange, which requires the datafication of the player's mobility and communicative actions. In exchange, the game offers privilege of access to its platform. At the same time, the authors note the standardization of surveillance and data mining contained in games such as Ingress. Unlike these commercial applications, we intend to use data mining not as a commercial viability item of our platform, but as a thematic element of the game. The same is true for camera surveillance and the integration of imaging data, which are exploited by their exposure and estrangement, not by their normalization.

Players and groups interact with the game and its proposed background story by inputting data 'inside the game' (among profiles of regis-

tered players) and 'outside the game' (among players and cameras soon to be mapped and inserted as playable elements). Mobile devices, from which the game are run, are also adapted and redimensioned. In the game plot, the DIO app is presented as a fictional hack, offering players a new way to control their smartphones. By 'shielding' DIO surveillance protocols and giving smartphone owners the power to act and resist in the global technology grid, smartphones become, in the DIO universe, technological re-appropriation devices and a political statement.

For players of both resistance groups, actions comprise a) registering and geolocating surveillance cameras scattered in public areas; b) fighting for 'ownership' of each of the logged cameras. To register and geolocate the camera, the player must approach the device with their mobile phone GPS activated and snap a picture, and, optionally, log in information as to where the camera is pointed (to a public or private area, for example) and its model.

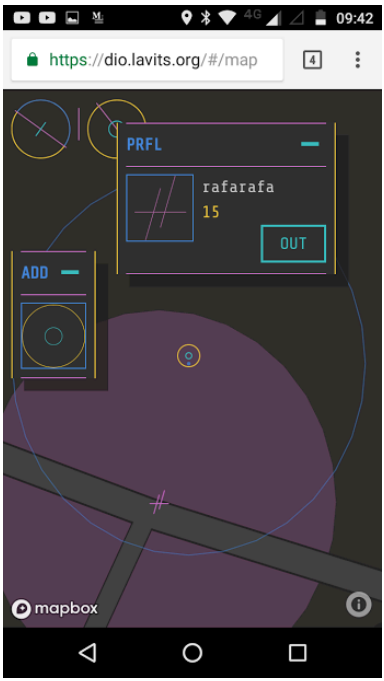

Figure 2 – Two cameras mapped by users.

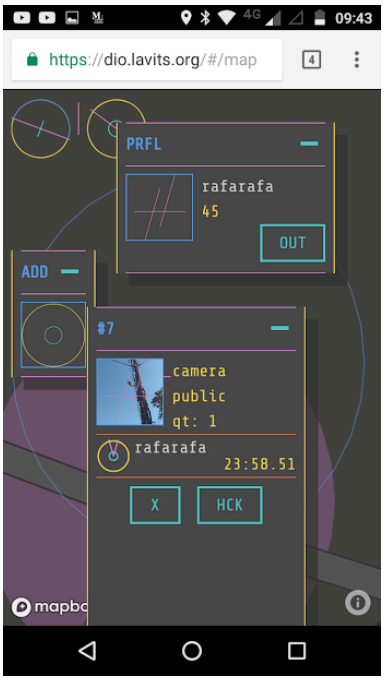

Figure 3 – Picture of mapped camera inserted by user.

To compete for the possession of the cameras, the player must have his/her GPS function activated and be within a radius of 50 meters of the

geolocated object, and then interact with it. Each interaction, which may be performed in predefined time intervals, increases your radius of control over the camera. For example, if the camera is under the control of the Lens group and a player from the Blind group goes through this area, Lens will lose points, and vice-versa.

The interaction, or the hacking of a camera by a team cancels the opposing team's interaction. Cameras/objects have a pre-set maximum radius perimeter that allows for interaction.

Game functions are still in development, and new implementations, adjustments, and tools are being studied.

The next two screenshots were taken using a mobile phone. Fig. 2 shows two mapped cameras: the closer to the street was hacked by a player and is in possession of his team. Fig. 3 shows a picture of the hacked camera, the time lapsed since the last hack and some information about the camera (a picture, the number of cameras, and if it is a directed towards a public or private area). Both also show some information about the player: his or her username, the number of points at that moment. The symbol right next to the user name shows that the player belongs to the Blind group.

5. Commercial Use of Personal Data

DIO is a MMOG. Each player has a username and accumulates points. Points permit the acquisition of new playable items that increase player potential, contributing to the wellbeing of the group.

When analyzing MMOGs, Kerr at al. (2014, 321) remember that "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". Our goal is to expose this kind of data collection, allowing for players explore their own data. For example, each user would be allowed to view the paths they took, on which days and times, and with which cameras they interacted. We must consider that this information may also be stored by other apps.

This functionality allows us to address the commercial use of personal data gathered through surveillance. In the same way we took into consideration the visibility of video surveillance devices in the game's context, we also intend to reveal how data gathering techniques are central to the operation of the game.

Commercial use of personal data on the Internet is constituted, just as surveillance cameras, as a controversial social issue that has been the subject of legislative proposals. It involves citizens (Internet service users); companies providing these services (that use data as raw material for intelligence analysis with commercial purposes); and governments (which use collected data to provide public services, political repression, and se-

curity practices).

It is estimated that by 2020, the market for 'digital identities' in Europe will sum up annual profits of up to 1 trillion euros (Boston Consulting Group 2012). Companies have made significant efforts to distance themselves from negative perceptions linked to governments and political surveillance. They intend to position themselves as having less power over citizens than our governments. They argue that, given freedom of competition, citizens are free to choose alternative services and that legislation's only function is to curb misuse and any eventual personal data leaks (Ashton-Hart 2014).

It can be argued, however, that migrating to other social network services is not that simple. "It's difficult for you to leave if all of your friends are members of a particular service, even if you don't agree with privacy settings changes," states Peter Schaar, Chairman of the European Academy for Freedom of Information and Data Protection (Schaar 2014). Another issue to consider are the astronomical profits projected by the information industry. Control and storage of personal data, which has been called the 'new petroleum', is a significant economic force that affects the global economy and, consequently, social relations. More than ever, information is power, as discussed by Ceglowski (2016):

> In our attempt to feed the world to software, techies have built the greatest surveillance apparatus the world has ever seen. Unlike earlier efforts, this one is fully mechanized and in a large sense autonomous. Its power is latent, lying in the vast amounts of permanently stored personal data about entire populations.
>
> We started out collecting this information by accident, as part of our project to automate everything, but soon realized that it had economic value. We could use it to make the process self-funding. And so mechanized surveillance has become the economic basis of the modern tech industry.

It is a difficult task to discuss and convince the public that their personal data has commercial value. Zuboff (2015) describes broadly the phenomenon and its logic of accumulation, calling it "surveillance capitalism". From the individual's perspective, data seems to be very trivial information. True concern only emerges with regards to sensitive data, such as bank account information, which can be stolen by criminals with the intent of illegally transferring funds (Firmino et al. 2011). Through its gameplay, DIO demonstrates what data can actually reveal about individuals, even if anonymously. More importantly, the game can show how personal data has become a tradable good. Accumulated data from other users means exponential profit growth. On the other hand, providing this information to others means losing power.

In a later stage of app development, new features that relate to this aspect may be implemented. One possibility is to create a system in which players exchange sets of information for game points (anonymously added according to playing time). The market for such exchanges wouldn't

be 'official', but game administrators would minimally regulate the nature of the exchanges.

Reward points would follow a nonlinear, exponential progression, thus emphasizing the value of being in possession of such vast databases. Similarly, gameplay for users with few points could be difficult, thus signaling that those who have amassed more information and more points have greater power and convenience.

These new features would be developed based on the actual characteristics of the personal data market. Therefore, by using the narrative features of the game, we would create a tool to discuss privacy and personal data.

6. Conclusions

There are several elements developed for the game that relate to current issues involving privacy, security, and power, such as the uncontrolled dissemination not only of cameras but of sensors capable of capturing information, as well as the indiscriminate data exchange between state agencies and private corporations. Even the differences established between the game's resistance groups – those that advocate for social control over technology, and those calling for radical disruption – echoes those of contemporary ideological currents.

The game story is still open. New elements may be added, along with new playable tools. Mobile phones have become powerful sensors that produce and transmit data continuously. This data is commercially used by technology companies (Evangelista 2016). We also intend to develop elements and playable items that portray this fact.

This project, in its complexity, from the development of the backstory and the coding of the game to the analysis of how the players are using the game, can be classified as a kind of sociological experiment. We are a group of independent academic researchers in the periphery of the info-industrial world. Using trends of the current game industry that emphasize different modes of surveillance seen in commercial games like Ingress (Hulsey and Reeves 2014, 389) and Pokemon Go, can we produce a game that challenges the surveillance culture? Canossa (2014) tells us about the growing trend among players towards unconditional acceptance of behavior tracking in digital games, and discusses the balance between the monetization of data generated by use and its compensation in different forms. How can we thematize surveillance capitalism (Zuboff 2015) and how will the players respond to that?

The game should be promoted initially in Latin America, in countries where there is a history of violation of human rights and where the institutions created to protect civil rights are recent and fragile. How will media, government and the public react to our effort to expose the location of public cameras? Are we going to be successful in our goal to increase

awareness about the surveillance structures of cities?

Besides that, there is also the amount of data that should be generated by the players. Could it be an opportunity to promote awareness about surveillance capitalism? How should we deal with that data? How much of it will we have to use to manage the gameplay? How should the consent policy to be established with the players be negotiated? How can we involve them in elaborating the terms of their consent? Kerr et al. (2014) show us that surveillant assemblages and governance, in flux, respond to and shape the behavior of players in MMOGs. Stenros at al. (2012) warn us about the challenges of studying pervasive games that blur the boundaries between play and everyday life. Not only are game data in a controlled environment involved, but also the cultural context and the daily life of players. In our case there is also the context of surveillance culture. We are only in the first moment.

References

ACLU (sd) *What's Wrong With Public Video Surveillance?,* https://www.aclu.org/whats-wrong-public-video-surveillance (retrieved June 28, 2016)

Ashton-Hart, N. (2014) *The Internet is not incompatible with data protection, but the debate we currently have about privacy largely is,* in W. Kleinwächter (ed.), *Multistakeholder Internet Dialog (MIND), Vol. 7: Privacy and Internet Governance*, Berlin, Internet & Society Collaboratory.

Barret, D. (2013) *One surveillance camera for every 11 people in Britain*, says CCTV survey, http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html (retreived June 28, 2016)

Ballard, J. G. (1997). *Which way to inner space*, in J.G. Ballard "A user's guide to the millennium: essays and reviews", New york, HarperCollins Publishers.

Barbrook, R. and Cameron, A. (1996) *The californian ideology,* in "Science as Culture", 6 (1), pp. 44-72.

Boston Consulting Group (2012), *The Value of Our Digital Identity,* Liberty Global.

Brighenti, A. (2009) *Artveillance: At the Crossroads of Art and Surveillance*, in "Surveillance & Society", 7(2), pp. 175-186.

Bruno, F. (2014). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade,* Porto Alegre, Sulina.

Canossa, A. (2014) *Reporting From the Snooping Trenches: Changes in Attitudes and Perceptions Towards Behavior Tracking in Digital Games*, in "Surveil-

lance & Society", 12 (3), pp. 433-436.

Capps, K. (2016) *Mapping "Pre-Crime" in Rio*, http://www.citylab.com/crime-/2016/08/mapping-pre-crime-in-rio/496553/ (retrieved October 17, 2017)

Cardoso, B. de V. (2012) *The Paradox of Caught-in-the-Act Surveillance Scenes: Dilemmas of Police Video Surveillance in Rio de Janeiro*, in "Surveillance & Society", 10 (1), pp. 51-64.

Carr, R.A. (2016) *Political Economy and the Australian Government's CCTV Programme: An Exploration of State-Sponsored Street Cameras and the Cultivation of Consent and Business in Local Communities*, in "Surveillance & Society", 14 (1), pp. 90-112.

Castells, M. (1996) *The Information Age: Economy, Society And Culture: The Rise of the Network Society (Vol. 1),* Oxford, Blackwell.

Ceglowski, M (2016) *The Moral Economy of Tech (Society for the Advancement of Socio-Economics Annual Conference)*, http://idlewords.com/talks/sase-_panel.htm (retrieved on March 30, 2017)

Clavell, G.G. (2011) *The Political Economy of Surveillance in the (Wannabe) Global City*, in "Surveillance & Society", 8 (4), pp. 523-526.

Ellul, J. (1964) *The Technological Society,* New York, Vintage Books.

Evangelista, R. de A. and Fonseca, F. (2016) *Reconhecimento e superação da exploração capitalista em redes criativas de colaboração e produção*, in **"**Liinc em Revista", 12 (1), pp. 25-39.

Felsenstein, L. (2013) *Explorations in the Underground 1964 – 1970*, http://www.leefelsenstein.com/?page_id=50 (retrieved on March 30, 2017)

Firmino, R.J. et al. (2013) *Fear, Security, and the Spread of CCTV in Brazilian Cities: Legislation, Debate, and the Market*, in **"**Journal of Urban Technology", 20 (3), pp. 65-84

Firmino, R.J., Kanashiro, M. and Bruno, F. (2011) *Social effects of data processing and regulation of personal data in Latin America,* Technical report, IDRC.

Graham, S. and Wood, D. (2003) *Digitizing Surveillance: Categorization, Space, Inequality* in "Critical Social Policy", 23 (2), pp. 227-248.

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State,* London, Macmillan.

Groombridge, N. (2002) *Crime Control or Crime Culture TV?*, in "Surveillance & Society", 1 (1), pp. 30-46.

Haggerty, K.D. and Ericson, R.V. (2000) *The Surveillant Assemblage,* in "The British Journal of Sociology", 51 (4), pp. 605-622.

Hulsey, N. and Reeves, J. (2014) *The Gift That Keeps on Giving: Google, Ingress, and the Gift of Surveillance,* in "Surveillance & Society", 12 (3), pp. 389-400.

Illich, I. (1973) *Tools for Conviviality,* Glasgow, Fontanna/Collins.

Introna, L. and Wood. D (2004) *Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems,* in "Surveillance & Society", 2 (2/3), pp. 177-198.

Jouvenal, J. (2016) *The new way police are surveilling you: Calculating your threat 'score'*, https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bcc-ac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.4778f686d571 (retrieved October 17, 2017).

Kayyali, D. (2016) *The Olympics are turning Rio into a Military State*, http://motherboard.vice.com/read/the-olympics-are-turning-rio-into-a-military-state (retrieved June 28, 2016)

Kanashiro, M.M. (2006) *Sorria, você está sendo filmado: as câmeras de monitoramento para segurança em São Paulo*, São Paulo, Unicamp.

Kanashiro, M.M. (2008) *Surveillance Cameras in Brazil: Exclusion, Mobility Regulation, and the New Meanings of Security*, in "Surveillance & Society", 5 (3). pp. 270-289.

Kelly, H. (2013) *After Boston: The pros and cons of surveillance cameras*, http://edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/ (retrieved June 28, 2016)

Kerr, A., De Paoli, S. and Keatinge, M. (2014) *Surveillant Assemblages of Governance in Massively Multiplayer Online Games: A Comparative Analysis,* in "Surveillance & Society", 12 (3), pp. 320-336.

Kitchin, R. (2014) *The Real-Time City? Big Data and Smart Urbanism*, in "GeoJournal", 79(1), pp. 1-14.

Koskela, H. and Mäkinen, L.A. (2016) *Ludic Encounters – Understanding Surveillance through Game Metaphors,* in "Information, Communication & Society", 19 (11), pp. 1523-1538.

Leszczynski, A. (2016) *Speculative futures: Cities, data, and governance beyond smart urbanism*, in "Environment and Planning A", 48 (9), pp. 1691-1708.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life,* New York, McGraw-Hill Education.

Luke, R. (2006) *The phoneur: mobile commerce and the digital pedagogies of the wireless web,* in P. Trifonas (ed.), *Communities of Difference: Culture, Language, Technology,* London, Palgrave Macmillan, pp. 185-204.

Marcuse, H. (2013[1964]) *One-dimensional man: Studies in the ideology of ad-*

vanced industrial society, London, Routledge.

Morozov, E. (2014) *To save everything, click here: The folly of technological solutionism,* New York, PublicAffairs.

O'Donnell, C. (2014) *Getting Played: Gamification, Bullshit, and the Rise of Algorithmic Surveillance,* in "Surveillance & Society", 12 (3), pp. 349-359

Rossman, M. (1972) *On learning and social change,* New York, Random House.

Sadowski, J. and Pasquale, F.A. (2015) *The Spectrum of Control: A Social Theory of the Smart City*, in "First Monday", 20 (7).

Saker, M and Evans, L. (2016) *Everyday life and locative play: an exploration of Foursquare and playful engagements with space and place,* in "Media, Culture & Society", 38 (8), pp. 1169-1183

Schaar, P. (2014) *The Internet and Big Data - Incompatible with Data Protection?*, in W. Kleinwächter (ed.), *Multistakeholder Internet Dialog (MIND), Vol. 7: Privacy and Internet Governance*, Berlin, Internet & Society Collaboratory.

Stenros, J., Waern, A. and Montola, M. (2012) *Studying the Elusive Experience in Pervasive Games*, in "Simulation & Gaming", 43 (3), pp. 339-355.

Sadowski, J. and Pasquale, F. (2015) *The spectrum of control: A social theory of the smart city*, in "First Monday" 20 (7). Available at http://papers.ssrn.com-/sol3/papers.cfm?abstract_id=2653860.

Thrift, N. (2014) *The "sentient" City and What It May Portend*, in "Big Data & Society", 1 (1), pp. 1-21.

Thrift, N. and French, S. (2002) *The Automatic Production of Space*, in "Transactions of the Institute of British Geographers", 27 (3), pp. 309-335.

Turner, F. (2006) *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism,* Chicago, University of Chicago Press.

Uchinaka, F. (2011) *Em uma década, número de moradias aumenta mais que o dobro que o crescimento da população*, http://noticias.uol.com.br/cotidiano-/ultimas-noticias/2011/04/29/em-uma-decada-numero-de-moradias-aumenta-mais-que-o-dobro-que-o-crescimento-da-populacao.htm (retrieved June 28, 2016)

van Brakel, R. (2013) *Playing with Surveillance: Towards a More Generous Understanding of Surveillance,* in "Proceedings of LISS conference 3", pp. 281-294

Viana, N. et al. (2017) *O que descobrimos – Vigilância*, http://apublica.org/-vigilancia/o-que-descobrimos/ (retrieved on June 28, 2017).

Vlahos, J. (2012) *The Department of Pre-Crime*, in "Scientific American", 306

(1), pp. 62-67.

Winner, L. (1997) *Cyberlibertarian myths and the prospects for community*, in "ACM Sigcas Computers and Society", 27 (3), pp. 14-19.

Zuboff, S. (2015) *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, in "Journal of Information Technology", 30, pp. 75-89.