Playing Spy Games: a Surveillant Platform Study of Microsoft's Xbox 360

by

Alexander Cybulski

A thesis submitted in conformity with the requirements
for the degree of Master's of Information

Faculty of Information
University of Toronto

Playing Spy Games: A Surveillant Platform Study of Microsoft's Xbox 360

Alexander Dean Cybulski

Master's of Information

Faculty of Information
University of Toronto

2014

Abstract

This thesis, a platform study of Microsoft's videogame console the Xbox 360, demonstrates how one of the defining traits of the videogame platform's design and architecture is pervasive surveillance of its users. By applying William Bogard's (1996) theory of surveillant "enclosures," this thesis will explain how the Xbox 360 uses a panopoly of methods and technologies to watch users and shape their use of the videogame system, forming them as easily governed subjects. In support of this argument, this thesis will examine not only the hardware and software layers of the Xbox 360, but also peripheral hardware and networks including the motion tracking sensor the Kinect and Xbox Live, the videogame console's online network. Of particular interest to this platform study will be an examination of how each of these layers performs surveillance, and how they collectively perform a project of governance over videogame players.

References

Bogard, William. (1996). *The Simulation of Surveillance: Hypercontrol in Telematic Societies.* Cambridge: Cambridge University Press.

Acknowledgments

This thesis sprang from a small class assignment: evaluate a specific technology and critique its privacy impact on users. What began as a class project turned into a thesis, a project which has taken two years to realize. Along the way many academics, professionals and friends have provided invaluable help in seeing this project through to its completion and to whom I owe a great personal debt. First and foremost, a thank-you to my committee, but especially to professor Leslie Regan Shade for talking me into writing a thesis, guiding me through this process and being a patient steward of my work. Special thanks are also in order for Joseph Ferenbok who introduced me to Surveillance Studies: your mentorship has had a profound impact on my work as an academic. My efforts on this thesis are in part due to the support I received from friend and comrade Patrick MacInnis who has always provided good conversation on thesis writing, grading, fear, loathing and deadlines – or – distraction from those topics altogether. Thanks to my technical advisors Mark Story Jr. and Matthew Wells for their advice on matters related to programming and software design. I owe a great deal to Jennifer Whitson who helped to push this thesis forwards and to Brenda McPhail for her confident words. Finally a special thank-you to my partner Jessica Dubeau, who has always provided a light in dark times and carried me when I needed support.

Table of Contents

Chapter 1

1.1 Playing Spy Games

On May 16th, 2014 Microsoft announced a curious decision: the Xbox One, the company's newest videogame system, would be sold without the second iteration of its motion tracking camera, the Kinect. The news was surprising for a variety of reasons: first, Microsoft had announced in numerous press releases and events that the Xbox One and the Kinect were a unified device, making the camera/sensor a mandatory component of the videogame platform (Tassi, 2014). Up until this announcement by Microsoft the configuration of the Xbox One and the Kinect meant that if a user wanted to play videogames with the device they would be forced to keep the always-on microphone and camera housed inside the Kinect connected to the videogame system. The previous decision to make the Kinect a mandatory component of the Xbox One had been met with tremendous skepticism and privacy concerns by consumers who were wary of installing a powerful, always-on biometric sensor in their living rooms (Gera, 2014). Secondly, this about-face from Microsoft regarding its policies towards the Kinect signaled a significant departure from its prior business plans: Microsoft had heavily invested in the Kinect, creating a revenue stream from data collected by it in the form of "nu-ads", which can basically be understood as recordings of consumers as they watch commercials (Trout, 2011).

Perhaps the removal of the Kinect signifies the price of data stewardship in the post-Snowden era, as organizations like Britain's Government Communication Headquarters (GCHQ) had proposed using the always-on camera and microphone inside Kinect as a method for spying on the living rooms of suspected criminals, or more likely, anyone caught up in dragnet style surveillance conducted by the English-speaking signals intelligence alliance colloquially referred

to as the ‘Five Eyes’ (Kain, 2014). It is also possible that the removal of the Kinect is an attempt to sidestep the quagmire of privacy concerns that have dogged Microsoft since the release of the Kinect in 2010 (Hollister, 2010). Additionally, Microsoft’s abandonment of the Kinect might have had something to do with Apple’s acquisition of Primesense, the Israeli company which owns the patents for the sensors used in the Kinect (Israel, November 25, 2013).

From a business perspective, the removal of the Kinect might indicate that the device simply wasn’t generating the revenue to justify its cost to the consumer as part of Microsoft’s overall business strategy. Removing the camera allowed Microsoft to drop the price of the Xbox One by $100 U.S. dollars, making it more competitive with platforms sold by Sony and Nintendo (Gilbert, 2014). While this latter explanation is compelling, the mostly likely scenario probably involves all four of these explanations, as they demonstrate not only the fiscal, but the political costs of deploying cutting-edge identification, tracking and recording technologies -- essentially those that constitute a high powered surveillance device -- into the homes of consumers.

However, surveillance is not constituted by simply cameras and microphones, although these devices are historically powerful symbols of the way in which the asymmetrical relationship between the watcher and the watched have been constituted. The presence of the Kinect is indicative of a much deeper power relationship between consumer and corporation: the notion that a user would willingly install a camera, which they cannot turn off, into their own home suggests that Microsoft has structured the experience of playing videogames in such a way that it is closely tied to conceptions of being watched and monitored. This relationship speaks volumes about the political economy of the contemporary home videogame system and the degree to which surveillance has permeated consumer electronics.

This thesis, a platform study of the Xbox 360, will examine the videogame console to demonstrate how surveillance and the control it permits are ubiquitous traits of the videogame console, present in the software, hardware and network architecture of the device. At the same time, it is important to recognize that the surveillance and control capacity of different components of the Xbox 360 do not always constitute a singular goal, but are instead indicative of different systems of governance which Microsoft has sought to implement to strengthen and protect its fiscal gains from the videogame system.

For example, few could argue that Microsoft's collection of data related to a user's game play through a system known as "achievements," could be connected to its efforts to defend against software piracy through a complicated system of anti-tampering protections in the hardware of the Xbox 360. However, both operations are constituted by different kinds of surveillance, and additionally both these initiatives allow Microsoft to generate or protect revenue made from the Xbox 360 in ways that will be examined in detail throughout this thesis. Primarily, this thesis argues that the Xbox 360 utilizes a polyphony of surveillant systems as forms of governmentality to shape the behavior of users, transforming them from players into subjects who are mined for data and ultimately, shaped by the gaze of the videogame system to suit Microsoft's financial interests. In support of this argument, this thesis performs a systematic analysis of the Xbox 360 as a platform, examining the device's history, its software, hardware, networks, policies and associated peripherals like the Kinect. One of the focal points of this thesis, will be the demonstration that Microsoft's efforts to surveil the user alters both the design of games and the experience of playing digital games in non-trivial ways which have important implications for the enjoyment of videogames and the artistry of their design, not to mention the political economy of videogame production and user privacy.

The question could be asked: why is Microsoft engaged in such extensive surveillance of its consumers? It is important to recognize that despite significant profits, the production of a videogame system is a risky enterprise. The home videogame industry has since its formative years experienced significant economic disasters, crashing in the early 1980s and since then the industry has faced considerable instability (Sinclair, October 3, 2013). Flagship institutions of the videogame industry like Atari, Sega, THQ, Ion Storm and Sierra Online have gone bankrupt or have had to significantly scale back operations. Numerous electronics industry giants have also tried their hand in the videogame console industry: Panasonic, Fairchild Semiconductor, Phillips Nokia, RCA, Magnavox, Pioneer, NEC and Apple Computers have all fielded failed videogame systems. Microsoft may soon find itself on that list. Despite relatively strong sales of its Xbox One since its release in 2013, the software giant has supposedly considered selling off its videogame division to buyers like Amazon (Fahey, February 28, 2014) and Warner Brothers (Tassi, August 17, 2014) due to the fact that its videogame console has not returned the profits expected from its first year on the market. These rumors underscore the importance of risk management in the videogame industry, as the companies which manufacture these sophisticated and expensive computers survive or fail on increasingly narrow margins in a market experiencing a decline in sales (Economic Times, December 23, 2013). Subsequently, predicting and shaping the interests of consumers is tantamount to successfully producing a contemporary videogame console in a highly competitive marketplace. Videogame console producers are well situated to capitalize on this prerogative with the current generation of networked videogame platforms, capable of monitoring user behavior in games, digital marketplaces and even on social networks like Facebook and Twitter. Consequently, this thesis will reflect the business interests of videogame console producers as they pertain to risk management by exploring surveillant

elements of the Xbox 360 videogame console and demonstrating how they are intertwined with Microsoft's financial objectives.

1.2 Scope

Due to the interdisciplinary nature of this thesis each chapter will rely on a variety of different methodologies for analyzing the various layers of the Xbox 360, illuminating the surveillant aspects of the component being analyzed. Because this thesis is written from the perspective of information studies, it will serve as a socio-technical investigation that will be technically rigorous, but abstain from excessively technical explanations of how the Xbox 360's systems operate. Conclusive reports about the technical details about Microsoft's videogame platform have already been documented in numerous programming and technical manuals written by game designers including Harbour (2010), hackers like Michael Steil (2005) and forensic technology investigations by Xynos, et al (2010), which have been cited in this volume. In building upon this knowledge, this thesis will craft conceptual threads between these manuals, by using the information provided by their authors to ascertain the purpose and meaning behind the design and functions of the Xbox 360 as they pertain to processes of surveillance and control.

Additionally, this thesis will not provide a broad study of how groups of users perceive representations of surveillance on the Xbox 360. For the most part, this valuable work has already been done by scholars, notably from Mikael Jakobsson (2011), who has written an extensive ethnography about playful interactions with Xbox 360's achievement system, with only a peripheral consideration of surveillance. Comparatively the aim of this thesis is to crack the software and hardware enclosure of the Xbox 360 and relate its components to familiar processes and narratives about surveillance common in high-tech consumer culture and critique these systems in doing so.

Another important question is: why analyze the Xbox 360? The Xbox 360 was not Microsoft's first videogame console the original Xbox, nor is it the company's most recent videogame platform, with the Xbox One having been released in November 2013. Without going over details covered extensively in this thesis, it is worth observing that the Xbox 360 was significantly more successful than its predecessor with 87 million units sold by 2013 as compared to the original Xbox which was released in 2001 and sold roughly 24 million units by 2006 (Microsoft, 2013). As discussed throughout this thesis, the financial success of the Xbox 360 can be attributed to the way in which Microsoft has sought to generate revenue from surveillant aspects of the device including game telemetry (chapter 3) and improved hardware security (chapter 5). Additionally, the Xbox 360 is much more like a contemporary networked technology than its predecessor. Historic forces including the dispersion of broadband and wireless technologies were more common during the Xbox 360's deployment than its predecessor. Accordingly, the Xbox 360 interfaces with broadband Internet in a way in which we are much more used to: the Xbox 360 downloads applications, plays streaming media and permits users to play multi-player games online, whereas its predecessor was really only capable of the former. The applications running on the Xbox 360 allow it to interface with Facebook, Twitter and a variety of other social platforms provided by Microsoft. To this extent, the Xbox 360 is significantly more integrated with the flows of data common to our current information economy and the surveillance environment which undergirds that economic system.

With respect to the Xbox 360's successor platform the Xbox One there is simply less to be known. Since being announced in 2005 the Xbox 360 was built, marketed, hacked, analyzed, repaired and written about for the last decade. Some of these processes like the hacking of the Xbox 360 have taken years of work from a huge network of individuals and it would be impossible to emulate the quality of their research by attempting to provide similar examinations

of the Xbox One exclusively for the purposes of this thesis. Further, much of the analysis in this thesis is based not only on the technology, but Microsoft as an institution, which has deployed this videogame system: this gives the Xbox 360 a relationship to a larger narrative about a multi-billion dollar software company and its history. To this end, a decade of press releases, trade-show presentations, software patches and company blogs all play an important role in describing how the surveillance systems encapsulated by the Xbox 360 functions and has functioned as a cohesive system of risk management.

1.3 Why Write a Surveillant Platform Study?

Surveillance Studies is still an emergent discipline within the social sciences and the humanities. Much of the research done by scholars interested in surveillance has sought to identify theoretical models of surveillance or to identify the sociological impact of surveillance. Focal areas within this field of study have also gravitated towards the behavior of governments governing their citizens, law enforcement/intelligence organizations collecting information on their adversaries, and corporations identifying/profiling customers. Until very recently few studies have focused directly on games or the platforms through which they are played. Tangentially William Bogard (1996) has analyzed simulation as a kind of surveillance, which is useful in analyzing the design of games which are themselves a kind of simulation. Similarly Anders Albrechtslund & Lynsey Dubbeld (2002), Matthew Cousineau (2011) and Jennifer Whitson (2013) have all analyzed the potential for games to act as surveillant tools. Whitson, in particular, has analyzed game structures within quantified data collection programs, providing a means of understanding how the fusion of surveillance and games can shape behavior.

Yet to date there have been few direct studies about how videogames and the videogame industry harnesses play and surveillance to change player behavior or to explicate the role

surveillance plays in the governance of a videogame system. A recent special issue on videogames published by the scholarly journal *Surveillance & Society* has done much to address this gap in the literature, with articles examining different forms of surveillance constituted in digital games including thematic representations of surveillance in game content (Andersen, 2014), the visibility and labor of live-streaming game performances (Walker, 2014) and governance of thousands of players in massively-multiplayer online games through surveillance (Kerr, De Paoli & Keatinge, 2014).[i] One entry in this volume is of particular interest to this thesis: Alessandro Canossa's (2014) article *Reporting from the Snooping Trenches* which describes important surveillance techniques used within the game industry and their application in game design (Canossa, p. 433-434).

Despite this focus most recent examinations of surveillance in videogames only deal with the technology and code at work in these systems tangentially without explaining with technical specificity how these systems operate. By embracing the "technically rigorous" aspect of platform studies forwarded by scholars like Ian Bogost and Nick Montfort (2009, p. 2), this thesis addresses a gap in the literature by directly analyzing software and hardware involved in surveillant processes on the Xbox 360, demonstrating how they process information and perhaps most importantly, mapping theories of surveillance onto these operation. Further, the holistic approach offered by a platform study is vital to understanding the role of surveillance on the Xbox 360, which is not encapsulated by any one system, but by a panoply of surveillant software, hardware and networks.

1.4 Challenges in Writing a Surveillant Platform Study

In dealing with surveillant systems present in a mass-market electronic device this thesis proposes analyzing processes which are by their very nature covert and surreptitious, meaning

that one of the challenges in performing a surveillant platform study of the Xbox 360 is identifying and revealing surveillant technologies and processes. Consequently, because this thesis proposes to peel back complex layers of code, hardware and design and packaging situated around the use of videogames it also obliquely addresses the ways in which users enjoy and interact with videogames that have become intertwined with surveillance. To this end, this thesis is an exercise in revealing hidden mechanisms which create meaningful but often opaque structures in games. However, this study also proposes to answer a question posed by many surveillance scholars: can being surveilled be pleasurable? What kind of pleasure comes from being watched? Why do users accept and enroll in surveillant systems found within digital games? Answering these questions in this thesis will derive primarily from a technical inquiry into surveillance, but one that also opens up the possibility of understanding the relationship between surveillance and play. Simultaneously the thesis challenges the political economy of the videogame industry, which relies on the high-tech spectacle of videogames and their opaque design to deflect serious questions about how these devices are used to collect information on and exert power over the users who take these devices into their homes.

One of the greatest challenges in writing an analysis of the surveillance performed by the Xbox 360 is indicating a relationship between the multifarious ways in which the device monitors the user and demonstrating a coherent purpose behind all of the tracking that occurs. In truth, the only simple answer is that all of the surveillance occurs on the device act as systems of risk management, implemented by Microsoft to diminish an array of financial and material threats posed by not only selling, but also managing the deployment of an expensive entertainment computer throughout its lifecycle (currently nine years) as a relevant profit generating commodity. This risk management agenda unites otherwise disparate systems of tracking present on Microsoft's second videogame console, providing continuity between the

third chapter's analysis of videogame code and chapter five's analysis of Microsoft's policies regarding the repair and service of the Xbox 360.

1.5 Key Terms

As previously mentioned, one of the challenges in writing a surveillant platform study of the Xbox 360 is unmasking and identifying practices within the videogame industry which corresponds with the surveillant processes that can be observed on the videogame console; similarly, identifying useful analytic frames emerging from games studies to talk about a videogame platform can be similarly elusive when working from the frame of Surveillance Studies. To this end, it is vital to define some important concepts derived from games studies and the videogame industry which will be central to the execution of this thesis.

1.5.1 Platform Study

A platform study is the holistic analysis of socio-technical systems, oriented towards an understanding of how specific computer systems shape the expression of media. Ian Bogost and Nick Montfort define platform studies as an investigation into the "relationships between the hardware and software design of computing systems and the creative works produced on those systems" (Bogost & Montfort, n.d.). While Bogost & Montfort have themselves authored a highly influential platform study of the relationship between the Atari 2600 and the videogames industry of the 1970s and 80s, the pair have suggested that other platform studies "may emphasize different technical or cultural aspects and draw on different critical and theoretical approaches" (Bogost & Montfort, 2009, p.2-3). Specifically, this thesis utilizes Surveillance Studies as a critical and theoretical approach to analyzing the Xbox 360 as a platform to assess how surveillance shapes the experience of playing games on the system and user experiences in owning the videogame platform.

1.5.2 Gamification

Gamification refers to the imposition of game-like structures and reward mechanisms in non-game contexts. While the concept of gamification is not particularly new, as many non-game activities can have game-like structures imposed onto them, the popularization of the term gamification comes from the increased application of game-like structures in new media, particularly in web 2.0 applications. Gamification has been used in schools (Sheldon, 2010), online shopping (Grayson, June 24, 2014) and a myriad of other contexts to imbue these non-game activities with a playful quality. As Jennifer Whitson has argued, the association of non-play activities with games is a technique designed to induce behavior change by associating desired behaviors with positive feedback mechanisms common to the structure of games (Whitson, 2013, p. 164). With respect to this surveillant platform study, gamification takes on a special meaning because it is also indicative of behavioral tracking mechanisms in the code of digital gamified activities which not only reward users for good behavior, but monitors decisions and behavior as an actuarial tool used to instantiate governance over the user. Much in the same way a game imposes rules onto the user, surveillant gamified contexts can impose and enforce rules by tracking player behavior.

Gamification is also commonly associated with the term “serious games”: typically, these are gamified contexts related to education, health or public policy (Quinn & Neal, 2008) where gamification is intended to improve information retention in learners and encourage positive associations with desired behaviors and outcomes determined by the game designer and institution deploying the game. As William Bogard might observe, the simulation of these contexts through games demonstrates a desire by institutions to regulate behavior preemptively, by simulating and enforcing desired behavior in a game context to ensure this behavior is carried over into normative contexts. Serious games instantiate political power that is “never center, but

rather what centers" (Bogard, 1996, p. 26) behavior by modeling simulated contexts in serious games and evoking a behavior change which carries from this controlled environment into the un-monitored, non-simulated world. Similar patterns in gamification and game design, have become associated with "social games" those games played through mobile devices and applications that run through social networking platforms like Facebook. As Casey O'Donnell has noted, social games are a particularly pernicious application of gamification because they use an "appointment" mechanism, wherein users are encouraged to 'check-in' periodically to a game through their Facebook profile. By leveraging this check-in mechanic, users are encouraged to form a habitual behavior which is then exploited when the game begins requesting real-world money for in-game items and bonuses that offer to provide further stimulation to the user (O'Donnell, 2014, p. 352). Ian Bogost has been an outspoken critic of this style of gamification, arguing that this practice should be reclassified as the creation of "exploitationware", which he suggests captures the intention of "gamifiers" who construct gamified contexts designed to pursue exploitative outcomes (Bogost, August 8, 2011). But what does gamification have to do with analysis of the Xbox 360? Chapters 3 and 4 deal directly with "achievements" and "gamerscore" Microsoft's digital trophies and scoring system which gamify the *mundane non-game experience* of playing all games on the videogame platform. These chapters describe how these systems inoculate users towards surveillance and are intended to shape behavior.

1.5.3 Game Telemetry

Game telemetry, a practice used to perform Game User Research (GUR), describes the generation of data about a player's behavior in a videogame through tracking systems enmeshed within a videogame or videogame platform's code (Canossa, 2014, p. 433). Much in the same way data from an airplane's black box might describe the operations of an aircraft's instrumentation, mechanical systems and the actions of the vehicle's pilot; game telemetry

describes the player's actions in response to the stimuli of games (Drachen, 2012). In 2005 the Xbox 360 was the first videogame system to standardize the implementation of telemetric systems on all games played across the platform, ensuring that all games played on the system generate data about user interactions. Game telemetrics are especially pertinent now that many videogame platforms are networked to the Internet and require this network connection to operate at their full capacity: when connected to the Internet a videogame system like the Xbox 360 transmits its telemetric data to Microsoft for the purposes of game analytics. As Alessandro Canossa has observed: game telemetrics on networked platforms have triggered a dramatic shift in the ability of game designers and publishers to track how millions of users engage with their games outside of the confined setting of laboratories and office buildings where traditional game testing and the monitoring of game play has traditionally occurred in the past (Canossa, p.435). The tracking of player data as it is created through game play has significant implications regarding the surveillant applications of this information, which will be specifically explored in chapter 2 of the thesis, which examines the code of the XNA framework (a piece of software) which collects data through games as they are played on the Xbox 360.

1.5.4 Game Analytics

The term game analytics refers to the analysis of data derived from game telemetrics and other efforts to monitor game play as part of GUR practices. In turn, game analytics are intended to optimize the design of games for user enjoyment, but also as a technique which analyzes "comprehensive user behavior data to drive revenue" (Nasir, et al, 2013, p. 4). Usually both of these objectives are in some way interrelated and herein lies the surveillant element of game analytics: the practice of game analytics leverages the power that comes from the monitoring of user behavior monitors to optimize the financial performance of a videogame through data driven design. In the 1970s, Atari was one of the first companies to perform game analytics, by

performing “field observations, surveys, questionnaires and focus groups” to determine how to best make and market games for its target audience (Canossa, p.433). Over time the practice has evolved to include users paid to “playtest” games and the use of laboratories like those deployed by Microsoft which perform intensive studies on how a user interacts with a game before its release to the general public (Thompson, 2007). Game analytics and critiques of this practice are the focal topic of chapter 3 and chapter 4 which consider how users are identified and profiled as by the Xbox 360 and its network, Xbox Live.

1.6 Organization of Thesis

While the component parts of the Xbox 360 have been engineered to operate seamlessly, this thesis will provide a logical dissection of the elements which constitute the platform’s surveillance, including: (1) the software and code running on the device, (2) the platform’s internal hardware, and (3) networks and peripheral technologies including the Kinect sensor and the Xbox 360’s internet connection Xbox Live. The structure of this thesis will roughly follow this segmentation of these layers, considering how surveillance is performed by each component and relating it back to the holistic functions of the platform, but its evaluation will do more than outline the technological systems at work on the device: it will also consider social elements of the videogame system including, but not limited to policies which govern users playing games on the Xbox 360, the writings of hackers who tamper with videogame systems, marketing materials and other texts that constitute the Xbox 360 as a socio-technical artifact.

This thesis is comprised of six chapters, which will provide some background for analyzing the Xbox 360’s analysis of its components and their surveillant capacity, but also an evaluation of the platform which has emerged from a distinct videogame and computing culture. The first introductory chapter will provide an outline of the argumentation, methodology and chapters of

this thesis. Additionally, the introduction will establish why a surveillant platform study of the Xbox 360 is an important scholarly endeavor by outlining how the research performed here contributes to the field of Game Studies and Surveillance Studies.

The second chapter will ascertain the rationale for analyzing the Xbox 360, first by evaluating contemporary theories of surveillance based on the writings of scholars in the field of Surveillance Studies to outline recent theories of surveillance and elaborate on how this process constitutes different forms of power and control. After considering contemporary theories of surveillance the second chapter will shift focus to examine recent writings related to surveillance in entertainment, art and media. Finally, the chapter will conclude by providing a brief historical analysis of the relationship between videogames and surveillance.

The third chapter of the thesis will examine a very specific surveillant process on the Xbox 360, its capacity to collect game telemetrics: data derived from game play and related activities. By examining software, code and the design of games on the Xbox 360, the thesis will begin to map theoretical explanations of surveillance to surveillant processes found in the software of contemporary videogames, specifically William Bogard's model of surveillant "enclosures" (Bogard, 2012, p.31). To this end, this chapter will examine how game telemetrics are performed on the device and how they are represented to the user as "achievements," digital trophies collected by players. One of the focal elements of this chapter will be a consideration and critique of how telemetric data extracted from game play is used to perform game analytics, the data driven optimization of games through data mining practices. This examination of game analytics will explain how companies like Microsoft use the data gathered through surveillant processes by their videogame console as a risk management tool.

The fourth chapter examines how user data is collected by Microsoft as part of a project to govern users as they interact with the Xbox 360 videogame platform. Specifically, this chapter will utilize the framework established by Philip Agre in his essay *Surveillance and Capture: Two Models of Privacy* (1994, p. 109) to explain how Microsoft coerces, entices and subtly imposes enrollment into a surveillant network upon users through a variety of tactics. Having established how Microsoft enrolls users into their tracking, this chapter will focus on how Microsoft uses data collected by users to profile their behavior and govern their use of the system, with specific consideration given to how Microsoft punishes users for violating policies and standards. The predominant focus of this chapter will be in explaining how surveillance alters and shapes playing games and their users, transfiguring them into data mines and reliable consumers respectively.

The fifth chapter will analyze the hardware of the Xbox 360 and will draw on research derived from the writings of security hardware vendors, hackers, amateur repair communities and digital forensic experts to map the relationship between the electrical components of the device to low-level software operations. Specifically, this chapter will examine the ways in which the hardware of the Xbox 360 has been secured against user intervention including intrusions like hacking and software piracy, but also against less malicious processes like repair. In doing so this chapter will evaluate the political economy of a contemporary videogame system, identifying how power situated in the hardware's design is used to control user agency. Additionally, this chapter will assess the role of peripheral technologies used in conjunction with the Xbox 360, notably the Kinect, a suite of powerful sensors which Microsoft uses as a biometric tool inside the user's home. This examination will be performed by considering a variety of actors and networks that contribute to the security and or insecurity of a contemporary videogame system.

The sixth and final chapter will provide a conclusive evaluation of the Xbox 360 as a surveillant videogame platform. The conclusion will consider the effect of the videogame platform's surveillance on its users, the videogame industry and the future of surveillance in videogames.

Chapter 2

2 Literature Review & Critical History: Surveillance and Videogames

Surveillance Studies is a broad field of scholarly enquiry that draws attention from an array of interdisciplinary scholars, making it thus challenging to sketch a conclusive analysis of its canon. Surveillance Studies is also an emerging area of enquiry, which is constantly being shaped by policy events like the scandal over the National Security Agency's (NSA) clandestine PRISM program (Greenwald, 2014, p. 18), a widespread electronic surveillance and data mining initiative, new technologies such as facial recognition and a variety of academic-professional collaborations.[ii]

This literature review focuses on the surveillant aspects of Microsoft's videogame system, the Xbox 360, analyzing articles which can help to explain the device. Videogame systems are multifarious platforms, the product of advances in software, hardware, the marketing of commercial products and the culture surrounding personal entertainment. The purpose of this literature review is to contextualize the object of analysis for this thesis, to provide the exposition necessary to critically examine the Xbox 360 not just as a computing platform, but as a cultural artifact that is the product of numerous sociotechnical systems. To the end, this literature review features three sections. The first section, in its focus on general theories and models of surveillance, will provide a strong theoretical foundation for this review. The second section will examine scholarly writings that link entertainment and surveillance, especially as it applies to digital games. This section is intended to explore how scholars have conceived of surveillance as part of entertaining experiences that subvert or enhance media, including videogames. The third section provides a critical history of algorithms and videogames, examining their intersections

with respect to the military computing complex and surveillance. Specifically, this history will evaluate the way in which culture has influenced videogames, addressing issues of both visibility and surveillance which have affected the way videogames are made, sold and played.

2.1 Recent Theories of Surveillance: Escaping the Panopticon

If Surveillance Studies has a point of inception it is likely Michel Foucault's critique of a series of letters authored by 18th century British philosopher and social reformer Jeremy Benthem, which describe a prison-structure known as the panopticon (Foucault, 2007, p. 200). This prison structure has been linked to concepts including coercion, control, and discipline, but mainly the panopticon has been identified as a useful theoretical model for understanding surveillance. The structure of the panopticon has been compared to political ideologies, the functionality of technology, and more generally it has been used to describe systems of social relations.

However, Foucault's writings have proven to be deeply complex and scholars have interpreted the panopticon in a multitude of ways. Recent theories which regard the panopticon as a model for understanding surveillance have predominantly rejected the prison as a useful way of understanding surveillance and in its stead many scholars have proposed alternative models, or focused on more generalized theories which conceive of surveillance as an attempt to manage probabilities. Scholars including Kevin Haggerty (2006), David Murakami Wood (2007), Greg Elmer (2012) and William Bogard (2012) have emphasized the way in which surveillance is a project to manage uncertainty and create political stability. These writings are important because they explain not only what surveillance is, but also how it can be understood as a gaze which is materially different from other forms of watching. Moreover, these writings on the panopticon are useful because of their broad theoretical nature: they demonstrate that Surveillance Studies

can be used to explain a complex range of phenomena, incorporating traditional notions of oversight along with algorithmic and economic systems.

Kevin Haggerty, in *Tear Down the Walls: On Demolishing the Panopticon* (2006) rejects the panopticon. Haggerty argues that as either a "model or metaphor" the concept of the panopticon has been "over-extended to domains where it seems ill suited," noting that "important attributes of surveillance that cannot be neatly subsumed under the 'panoptic' rubric have been neglected" (Ibid, p. 23). While Haggerty's central thesis itself is not a turning point for Surveillance Studies, his argument does signify an important and necessary change within the discipline: a growing recognition that the dominant model for the discipline is becoming outmoded and ineffective as a means of exploring the subject. Haggerty notes the plethora of arguments made by scholars who modify the panopticon as a necessary means of explaining their work (Ibid, p. 23). Based on these shifts and modifications in the way surveillance is conceptualized Haggerty suggests that anomalies in surveillance have increasingly been difficult to accommodate with a panoptic model and subsequently a new model or a paradigm shift is necessary for more meaningful inquiries into the subject (Ibid, p. 23-24). However, Haggerty is also weary any dominant new singular model for understanding surveillance, noting that "surveillance, as manifest in the multiplication of its aims, agendas, institutions, operation forms, objects and agents… has become profoundly difficult [to define]" (Ibid, p. 41).

Instead of abandoning Foucault entirely, Haggerty points to the author's writings on governmentality, not as a new model to replace the panopticon, but as a process oriented form of institutional analysis which could benefit Surveillance Studies. To this end, Haggerty proposes that studies of "governmental projects" (more generally, institutional projects) could provide a much needed ambivalent and "normative stance to changes in the dynamics of power" (Ibid, p.

40). Evaluating this form of study, Haggerty notes that such projects are usually attempts to "persuade, entice, coerce or cajole subjects to modify their behavior in particular directions, the targets of governance are understood to be a locus of freedom… the emphasis on active agents suggest that all governmental projects entail opportunities for resistance, avoidance or subversion" (Ibid, p. 40). Haggerty thus alludes to the possibility of expanding Surveillance Studies to consider not just a model which facilitates the gaze, but rather systematic analyses of institutional processes which collect, structure and predict the data of subjects in order to manage their behavior.

This approach to governmental behavior adapted by Haggerty from Foucault emphasizes the role of probabilistic projects aimed at collecting data and managing populations. Evoking British sociologist Nikolas Rose (2006), Haggerty notes that studies of governmentality are often concerned with how institutions engage in "certain ways of seeking to act upon the conduct of others" or more simply, how governments understand their own efforts to affect the behavior of subjects (Ibid, p. 41-42). In making these observations, Haggerty notes that this methodology is dominated by discourse analysis and finds that it "[forgoes] important lines of inquiry into the actual experience of being subject to different lines of inquiry into the actual experience of being subjected to different governmental regimes" (Ibid, p. 42). Because of these deficiencies Haggerty envisions the role of Surveillance Studies as a discipline which injects empiricism into the study of governmentality, analyzing both the politics and experience of surveillance. This argument carves a niche for Surveillance Studies, one which seeks to understand how power is internalized and hidden within a "disciplinary society" (Ibid, p. 42).

Many of Haggerty's concerns regarding Foucault are echoed closely by his colleague, David Murakami Wood, in *Beyond the Panopticon: Foucault and Surveillance Studies* (Murakami

Wood, 2009). Here Murakami Wood questions whether further inquiry into Surveillance Studies can be sustained with a framework situated in Foucault's *Discipline and Punish* (Ibid, p. 2). Summarizing and compressing a significant amount of scholarly writing on Foucault, Murakami Wood suggests that the ideal site for the panopticon is no longer a spatial location and instead proposes that the database has become its most useful realization of the model: a space where identities are created and individuals are turned into "performative machines" (Ibid, p. 16). While it is categorically incorrect to say that the database is not a place (the storage and architecture of information has its own spatiality and location), Murakami Wood, similar to Haggerty, identifies how surveillance has become an act of information management, but is doubtful that Foucault himself would have thought of such file systems as panoptic (Ibid, p. 16). Herein lies Murakami Wood's grievance with Foucault, noting that the author's limited interest in digital technologies and his "Franco-centrism" severely diminishes *Discipline and Punish* as having continued relevance to a growing discipline like Surveillance Studies (Ibid, p. 16-18). In this respect, Murakami Wood argues that his discipline is becoming increasingly disassociated with a text which has historically been central to its theoretical foundations.

Moving beyond Foucault, Murakami Wood proposes that the best way forward for Surveillance Studies is to adopt the theoretical locus forwarded by French scholar Gilles Deleuze (1992) in his essay *Postscript on Societies of Control* and his concept of "control societies" to subsume the role of the panopticon (Ibid, p. 18). Dispensing with discipline as the central mode of the panoptic model, Murakami Wood notes that the concept affords little flexibility and alternatively he offers the concept of control, which he notes is both "digital and modulating," a social force which operates with granularity (Ibid, p. 18). Guiding lives within the control society, Murkami Wood suggests that individuals have become "dividuals" with their identities and bodies subsumed by multiple entries into a database, with this information subject to the

"dispositif": the mechanisms of power that sustain various institutions and governments (Ibid, p. 18). What can be understood from Murakami Wood's argument is that he envisions the alternative to the panopticon as a system which atomizes the individual into an array of data points and leverages the apparatuses of the institution to control the lives of each individual based on this information. This approach to social control suggests that societies are governed by a form of managerialism which turns individuals into pieces of information that guide and perform certain transactions necessary to sustain political stability.

Examining Murakami Wood's argument with respect to Haggerty's, certain congruities present themselves. Both scholars reject the panopticon as a model which has been stretched beyond useful limits. In this way, both Haggerty and Murakami Wood take a similar approach to the failure of the panopticon, but come to different conclusions: Haggerty believes the panopticon is beginning to fail as a model, which can be understood when he suggests that the panopticon is constantly being stretched to incorporate new surveillance anomalies. Comparatively, Murakami Wood suggests that the model was always too limiting, arguing that it has stunted the development of Surveillance Studies, evinced in his critique of Foucault. Moving forward, both scholars advocate a top-down analysis of institutional systems of governance, with Haggerty emphasizing the exercise of power as surveillance, while Murakami Wood focusing on the sorting and collection of information; surveillance as a power which creates and organizes information.

In *Panopticon - Discipline - Control* Greg Elmer (2012) argues that both Murakami Wood and Haggerty have largely derived their understanding of Foucault from the writing of Gilles Deleuze and in doing so, they have inadvertently adopted the French scholar's conflation of Benthem's writings with Foucault's critique of Benthem (Ibid, p. 21-22). Elmer argues that as a

result, Surveillance Studies is oriented towards an analysis of panoptic structures, failing to fully appreciate the coercive and disciplining effects of the panoptic gaze: its consequences for those being watched (Ibid, p. 23). This can be understood when Elmer suggests that Surveillance Studies has focused on the prison, rather than the prisoner, noting that Foucault saw panoptic surveillance as a form of institutional coercion, "the process of managing and governing the future" (Ibid, p. 23). What is significant about Elmer's argument is that he challenges existing Surveillance Studies literature to define surveillance not as a process which generates responses from its gaze, but to define surveillance as an act which sees the gaze itself as a form of control, one which is inherently restrictive.

Having defined surveillance as an act of coercion, Elmer explains how it is exercised through a political economy of the panopticon. For Elmer, the panopticon is power "reduced to its ideal form; its functioning abstracted from any obstacle, resistance or friction… a pure architectural and optical system: it is in fact a figure of political technology" (Ibid, p. 23). This economy is essential to Elmer's argument, as he defines the panopticon as not simply a structure for observing, but rather a figurative system which couples probabilistic methods with the removal of certain boundaries that permit the constant exercise of power. Contrasting the political objectives of Benthem and Foucault to strengthen his position, Elmer notes that the former saw the panopticon as a freedom from institutional violence which was originally needed to keep a prison functioning, identifying Benthem as a liberal visionary of prisons. In this way, the panopticon represented to Benthem a symbol which suppressed the need for violence (Ibid, p. 22). Comparatively, he argues that Foucault saw the panopticon in much more general terms, as "an internalized power that seeks to pre-plan, to economy the past, present and future" (Ibid, p. 25). In this way, Elmer depicts Foucault as a scholar interested in how power managed

probabilities, and how the panopticon was a figural process which created and expanded power. Elmer describes three criteria for disciplinary mechanisms as elucidated by Foucault:

> 1) Search for lowest possible cost both economically and politically speaking
>
> 2) The extension and intensification of its power and scope in an effort to avoid failure
>
> 3) To link the economic growth of disciplinary power with institutional output to increase both the docility and utility of all elements of the system (Ibid, p. 25).

This critique of Surveillance Studies departs from an architectural model of the panopticon limited by its need to signify specific actors, rather than an automated process which subsumes power based on a "probable gaze" (Ibid, p. 28).

Positioning Elmer with respect to Haggerty and Murakami Wood, it can be understood that he too identifies surveillance as a system which identifies probabilities and manages certain commodities to prevent risk. However, unlike both Haggerty and Murakami Wood, Elmer does not reject the panopticon as his political economy of the model suggests that it is particularly useful as a figurative mode of understanding the self-sustaining mechanisms of power. This argument carries a certain resonance with history, as it demonstrates how surveillance builds up over time, becoming an encompassing tool, effective for managing risk which might threaten the stability of growth. Elmer's argument is also simply more elegant than either Haggerty or Murakami Wood's, relying less on complex theories that incorporate a host of interpretations surrounding Foucault and instead, embracing a free-standing logical system.

Focusing on the spatiality of models for surveillance, William Bogard rejects the panopticon as an idealized model for surveillance and instead evokes French theorist Jean Baudrillard to suggest that the best model for understanding surveillance is the simulation. In *Simulation and Post-Panopticism (2012)*, Bogard argues that the panopticon is simply a "strategy of

representation" which attempts to signify the presence of an enveloping gaze (and the power that comes with being able to watch in totality) while simultaneously making the presence of the gaze unverifiable (Ibid, p. 31). This understanding of the panopticon is rooted in a spatial model which conceives of the watcher having maximum vantage over a subject(s) who cannot tell if they are being watched. However, this representative model for surveillance is untenable for Bogard as he notes it is prone to creating confinements: spaces which have boundaries that naturally obstruct the gaze and therefore act as spaces where opposition to this watching power can exist or foment (Bogard, p. 31). This allusion to the shortcomings of the panopticon can be understood as his critique of an architectural model, limited by a spatiality rooted in perspective: trying to watch all angles at the same time proves untenable. He concludes that the panopticon fails because it is an imperfect "enclosure" (Ibid, p. 31). As Bogard conceives of it, the panopticon cannot mitigate risk in its totality because it permits uncertainty in its failure to completely envelope the subject. In this way, Bogard demonstrates that the panopticon cannot be held up as an idealized model of surveillance because it is insufficient in managing probabilities.

To supplant the panopticon, Bogard suggests that the best model for surveillance is the simulation, an enclosure which does not rely on confinement and therefore permits the constant flow of information without "material constraint" (Ibid, p. 31). As Bogard suggests, the "enclosure" of the simulation, and not the "confinement" of the panopticon, can explain the expansion of surveillance in a period of "greater mobility of labor, speed of communication and risk management," what Bogard calls "modern productive forces" (Ibid, p. 31). Instead of confined modes of information gathering, Bogard notes the new tools of surveillance including "statistical modeling," "risk assessment," and "profiling, data mining and financial speculation" orient the control element of surveillance around access to information (Ibid, p. 33). This understanding of simulation as a form of surveillance rooted in prediction and managing

probabilities emphasizes the often ephemeral control of surveillance, rather than the panoptic model which must accommodate force necessary to confine an individual to a spatial gaze. By placing this emphasis on the collection of information, Bogard finds a more expansive model for surveillance less rooted in institutional violence of the prison but one that provides new problems of discrimination, ubiquity and social sorting.

Bogard's model of surveillance in the simulation is highly compatible with Murakami Wood's understanding of "dividuals" in a control society. Both Bogard and Murakami Wood emphasize the importance of modulation as the variable control which transforms multiple data-points into a coherent, probable system which allows for the mass control of individuals. In comparison to Elmer, both scholars envision the ideal operating conditions for surveillance to exist without boundaries to power and in this way, argue that the simulation might supercede the political economy of the panopticon, as this spatially grounded prison model describes the exercise of power as a force which arrests and confines growth. By contrast, within a simulation growth and development are the intended outcome; simulated processes are interested in change and movement rather than the confinement of the panopticon. Bogard's writings on the simulation are therefore useful, because it can account for the historical growth of institutions alongside its efforts in surveillance.

These writings on the panopticon inform an important theoretical debate within Surveillance Studies, which seeks to understand under what conditions surveillance can exist and what it might be used for. While the panopticon was rejected by a majority of the scholars analyzed in this section, these criticisms do not mean that this model is invalid when it appears in the works of other scholars, merely that its role in various arguments should be evaluated to understand its suitability. More importantly, these arguments demonstrate that surveillance is more than an act

of watching: organization, representation, probability and management play important roles in Surveillance Studies as well. In addition, institutions are clearly a factor in how surveillance is performed, as demonstrated by a dominant trend in these writings in their consideration about what processes might be exercised or embodied within the structures of organizations. Surveillance is often conceived of as a clandestine operation and while its treatment by scholars has ruminated on pervasive conceptions of surveillance all of these authors have also demonstrate how the exertion of coercion, control and discipline is often masked by certain forces -- some deliberate and others circumstantial.

2.2 Surveillance as Entertainment: Art, Games and Ubiquitous Computing

In his book *the Four Fundamental Concepts Of Psychoanalysis* (2012) and other writings French psychoanalyst Jacques Lacan has emphasized that the gaze can be a pleasurable and even entertaining experience for the watcher (p. 70). Building from this concept Surveillance Studies has identified a panoply of gazes, explaining the different ways in which the watcher might conceive of their subject, but additionally how the subject might conceive of their own surveillance. More importantly it is the Surveillance Studies discipline which has ascribed a socio-political value including the power of the gaze and the potential harm it can cause, giving meaning to surveillance through analysis of the gaze and its effects. The vast discrepancy between the Lacanian gaze and the surveillant gaze criticized by Surveillance Studies is reason enough to interrogate such a conceptual gulf: can surveillance be a pleasurable, fun activity? Or does its social harm outweigh its novel entertainment value? Given the relative youth of Surveillance Studies as a discipline and its political imperative to criticize surveillance practices, it is perhaps unsurprising that analysis of surveillance has been soberly focused on its controversial nature, rather than on its potential as a medium for entertainment. As this chapter

has sought to describe, new directions for surveillance are rapidly opening as old models for understanding the practice are being outmoded. As this opinion has shifted, an emerging body of work has been produced documenting the application of surveillance in art, games and other entertainment media. As this section of the literature review will demonstrate, scholars studying surveillance as entertainment are particularly disruptive to traditional models of surveillance, because they demonstrate how the surveillant gaze is modulated in its intensity and style through various relationships, challenging traditional notions of coercion and control often associated with a surveillant gaze. These writings on surveillance as entertainment are therefore important, because they provide a logical explanation of how surveillance, and the opportunity to be surveilled, can be a seductive and even pleasurable experience.

In their influential 2005 article *The Plays and Arts of Surveillance* Anders Albrechtslund and Lynsey Dubbeld note that while the study of surveillance practices has been "dominated" by the discussion of its negative implications, an examination of surveillance's caring and enabling applications is long overdue. Answering a call from David Lyon, a leader in Surveillance Studies, to recognize "the Janus faced" nature of surveillance, Albrechtslund and Dubbeld examine games and art to determine how surveillance can be a "playful, amusing and enjoyable practice" (Ibid, p. 217). While the concepts surrounding surveillance have appeared in popular works like George Orwell's novel *1984* (Orwell, 1949) or Francis Ford Coppola's 1976 film *The Conversation* (Coppola, 1976) as a thematic element, Albrechtslund and Dubbeld suggest that richer and more diverse examples can be found in media which entertains through the act of surveillance (Ibid, p. 218). As both scholars note, media which thematically addresses surveillance with any depth tends to be limited, focusing on more controversial aspects of surveillance, rather than examining the practice conclusively (Ibid p.218). Albrechtslund and Dubbeld's focus on media which utilizes surveillance as part of its production or as a perspective

within a medium is thus sensible: analyzing the relationships created by surveillance entertainment and its impact is more in line with the goals of Surveillance Studies than a thematic orientation towards the study of film or literature.

Performing a cursory examination of popular media utilizing surveillance in 2005, Albrechtslund & Dubbeld analyze a version of the popular board game Monopoly that tracks cab drivers in London, and an art installation which gathers and organizes surveillance footage into visually enticing patterns. Based on these experiences, Albrechtslund and Dubbeld note that internet communication and networked technologies can facilitate engaging and interactive media: "producing excitement and diversion" by utilizing surveillance in novel ways (Ibid, p. 219). A quality shared amongst the media analyzed by Albrechtslund and Dubbeld are artworks and games which exploit the networked nature of our technology and society to collect disparate pieces of information and organize them into coherent, amusing relationships. This argument shares many similarities with that made by David Phillips in his essay *Ubiquitous Computing, Spatiality, and the Construction of Identity*, wherein he argues that within certain spaces, surveillance can facilitate a variety of previously inaccessible interactions (Phillips, 2009, p. 33). Instead of the safe and commercially viable urban landscapes which feature prominently in Phillip's article, Albrechtslund and Dubbeld see a dearth of media experiences made possible through surveillance. Their argument is thought-provoking, as it suggests that there is a social element to these experiences that is otherwise elusive to non-surveillant experiences.

Despite their cursory treatment of surveillance and entertainment phenomena, Albrechtslund and Dubbeld's conclusions from these experiences are perhaps the most significant part of their article. First, they allude to the pleasure of the gaze but also note how this perspective can be problematic: among their examples, they suggest that most of these experiences offer a fairly

unproblematized exhibition of surveillance for consumers (Ibid, p. 219). They further conclude that future scholarly analysis of surveillant media is important to understand if the security industry is permeating media, and to better understand how the use of surveillance can allow individuals to become more sensitive to the presence of surveillance (Ibid, p. 220). Second, they suggest that the presence of surveillance in entertainment is disruptive to dominant surveillance metaphors and models, including "Big Brother" or the panopticon, as the mode of surveillance found in entertainment is often more horizontal, rather than the traditional top-down oversight. While their conclusion is that further research is necessary, their arguments are in line with those made by Haggerty and Murakami Wood, who observed that the panoptic model was becoming outmoded. This research thus highlights the shifting discourse of Surveillance Studies observed by other scholars and establishes a need for further investigations into pleasurable modalities of surveillance.

Focusing more narrowly on contemporary art which features surveillant elements, Andrea Mubi Brighenti in *Artveillance: at the Crossroads of Art and Surveillance* (2009), analyzes the concepts of visibility and recognition to understand how these shifting ideas play an important role in the relationship between surveillance and entertainment media. Art, Brighenti argues, can serve as a method of interrogating surveillance, while simultaneously being influenced by surveillant practices. Brighenti calls this process of interrogation "Artveillance": the examination of "reciprocal influences and exchanges between art and surveillance" (Ibid, p. 175). Brighenti argues that there is a certain cultural exchange taking place, with surveillance influencing art. To understand these reciprocal phenomena, Brighenti interrogates the concepts of visibility and recognition to identify distinct modalities which inform our understanding of these terms (Ibid, 176). In particular, Brighenti is interested in how visibility and recognition constitute social relationships which shift as an individual interacts with external agents including the public and

the state, suggesting that this alters how surveillance is perceived and understood by individuals. This argument is similar to Murakami Wood's recognition of the digital nature of surveillance, suggesting that the surveillant gaze is capable of modulation, a change which occurs contextually as the visibility and recognition of an individual shifts with their environment.

Focusing on visibility and recognition in public space, Brighenti notes that among street art (graffiti artists) in Europe there is a certain recognition of how surveillance has become ubiquitous within public space. In this way, she notes that many artists have sought to subvert the constant gaze of cameras by putting up their own illustrations of cameras in discrete locations, aping the "asymmetric visibility created by the practice of control" (Ibid, p. 178), a practice she suggests is a reply to the pervasive gaze of surveillance cameras in Europe. While Albrechtslund and Dubbeld focused on street art that utilized the technology of surveillance, what is interesting about Brighenti's arguments is that she suggests that surveillance is more than a technology, but also a political style with its own rhetoric. In this instance, the visible rhetoric of street art is significant to Brighenti's argument about surveillance art's subversion of the gaze; these images of surveillance technologies co-construct a social space, the city, with its population. Therefore, what is important about Brighenti's selection of art is its public rhetoric which contrasts the "Sorting Daemon" installation analyzed by Albrechtslund and Dubbeld, an exhibit that worked surreptitiously and secretly and in doing so evaded the logic of surveillance that not only watches but shapes its subject (Albrechtslund & Dubbeld, p.217). This distinction in selection is important because it demonstrates that Brighenti is not merely focused on art with the "theme" of surveillance, but that she analyzes an art form which espouses the rhetoric of surveillance. Subsequently, selection and evaluation of rhetoric is one of the strengths of Brighneti's work, as her exploration of surveillance as an artistic motif among a variety of artists reveals certain commonalities in their perception of surveillance.

Brighenti's argument does much to develop Albrechtslund and Dubbeld's original thesis, suggesting that while elements of surveillance culture influence a medium, it is possible for the same medium to intervene against and protests surveillance by adopting its pervasive logic. A similar argument has been made by Dan Trottier in *Crowdsourcing CCTV Surveillance on the Internet* (2014), wherein he observes that CCTV companies in Britain are turning to gamification (the process of making labor into a game), as a way of crowdsourcing the closed-circuit television surveillance of public spaces in the United Kingdom. In this way, the arguments made by Trottier and Brighenti bring surveillance and media into the same continuum, wherein elements of the production that constitute the creation of certain cultural products are shaped by experiences gleaned from other cultural products. Crowd sourcing and gamified surveillance can be understood to challenge the panoptic model as a form of representation and as representative labor. As a form of labor, gamified surveillance subverts its traditional relationship with security: the surveillant gaze is given so little value that it is outsourced for prizes, rather than pay. As a form of representation, the labor of gamified surveillance unmasks the work of the surveillance as mundane, challenging the high security connotations of surveillance implied by CCTV cameras as tedious work, subject to fallible operators. As Brighenti suggests, this kind of surveillance is unsurprising given the "haptic" (Ibid, p. 185) nature of the surveillant gaze, as it rationalizes a culture of surveillance making it accessible rather than impermeable, subtly normalizing surveillance within our society. It can be understood from Brighenti and Albrechtslund and Dubbeld's analyses that surveillance is subversive in the way it permeates media and that any surveillant elements in games and art should be analyzed to understand the property of surveillance that allows it to blend into the architecture of our experiences.[iii] While Brighenti is comfortable concluding that the relationship between art as surveillance is

ambivalent, her essay raises important questions about the way surveillance has a tendency to normalize itself as it infiltrates media, an issue similarly raised by Albrechtslund and Dubbeld,

Building on the reciprocal relationship noted in the works of Brighenti and Albrechtslund and Dubbeld, Matthew J. Cousineau argues in *The Surveillant Simulation of War* (2011*),* that war games are increasingly responsible for domesticating surveillance technology, and that surveillance technologies are increasingly resorting to familiar domestic technologies to improve surveillance labor. Central to Consineau's argument is the association between surveillance and violence, suggesting that the domestication of surveillance normalizes the violence performed by the military industrial complex, making it appear routine and acceptable rather than exceptional and morally questionable (Cousineau, p. 517). Cousineau draws heavily from Bogard's *The Simulation of Surveillance* to examine how entertainment developed by the American military is intended to predict and seduce potential recruits by simulating war, relating it to their hobbies and sensibilities (Ibid, pp. 518-519).

Of particular interest to Cousineau is how the American military increasingly presents their work as a game, designing realistic, but easily accessible simulations, including its infantry combat in the videogame *America's Army* and "America's Army Experience Centre", a glass-walled exhibit set up in malls where individuals can play with various combat vehicle simulators, an experience not unlike a videogame arcade common to malls in the 1980s and early 1990s (Ibid, p. 19). As Cousineau suggests, these entertainment experiences utilize the experience and enjoyment of young men playing videogames, what he calls "the embodied cultural capital" (Ibid, p, 519) to attract potential recruits to the military by conflating their ability with games as a predictor of their success within the military. However, Cousineau believes that the role of these simulations are twofold, in that they are intended not only to act as recruitment

propaganda, but also as a tool to indoctrinate the public by making simulated surveillance and the violence that it produces mundane and domesticated. This argument is significant, as it not only builds on Albrechtslund and Dubbled's earlier argument that surveillance is often presented un-problematically in entertainment, but it also implies that it is possible to make the violence that results from surveillance banal.

Considering the influence of entertainment media on surveillance, Cousineau notes that the U.S. military contracted the Harris Corporation, a civilian organization, to build a searchable video database for drone operations, similar to those it had designed for major sports broadcasters. As Cousineau suggests, this project, known as FAME, was intended to produce "highlight reels" of drone-strikes and surveillance intelligence, allowing users to quickly tag and organize information collected by remotely manned aerial drones (Ibid, pp. 519-520). Cousineau's analysis of this database implies that he views this technology as an adaptation of domestic technology, both as a way of easing surveillance work but also as a way to better organize war propaganda efforts, making the work of drones routine while simultaneously using this realistic information to feed back into simulations of drone operations to improve simulations (Cousineau, p. 520). In many ways, this argument mirrors Trottier's analysis of gamified surveillance systems in the UK, acknowledging how domestic technologies turn forms of labor that were once specialized into fairly routine and simple tasks. Applying the framework of Bogard's surveillant simulation, it can be understood that Cousineau views this system as self-perpetuating, making more realistic simulations by further expanding the conditions necessary to create a broader simulated enclosure.

Despite Albrechtslund and Dubbeld's promise to focus on the pleasurable aspects of surveillance, scholarship which has drawn from their work, including those of Brighenti and

Cousineau, have generally failed to explain *how* surveillance could be a pleasurable experience in entertainment. Instead they have maintained the dominant critical tone of Surveillance Studies towards its application, rather than its purpose. This is understandable, because as Jennifer Whitson argues in *Gaming the Quantified Self*, Surveillance Study scholars cannot accurately respond to surveillance in entertainment media until they properly comprehend how these experiences are pleasurable, and how "surveillant technologies are leveraged" for enjoyment (Ibid, p. 164). Whitson's argument addresses an important gap in the literature surrounding surveillance and entertainment; while it can be gleaned from Brighenti and Cousineau that some forms of entertainment utilize or embody surveillance, to date scholarship has yet to fully address *why* these experiences are pleasurable.

Drawing on the work of John McGrath in his book *Loving Big Brother* (2004, p. 2), Whitson notes that the dominant framework of Surveillance Studies is situated in crime control and privacy, inherently structuring and limiting "how we perceive, talk about and respond to surveillance" (Ibid, p. 164). Whitson instead suggests that seduction and desire play an important role in a new era of surveillance. This argument is significant as it challenges the traditional paradigms and boundaries of Surveillance Studies. The thrust of Whitson's essay is also evocative of Haggerty and Ericson's description, in their essay *The Surveillant Assemblage* (2000), of why consumers willingly submit to certain forms of surveillance. As they observe, consumers are increasingly seduced into providing the details of their lives, as reconstructed through their transactions, rather than through a typical panoptic model of coercion (Ibid, p. 615). They suggest that this is not a typical panoptic relationship, as the consumer does not train or discipline themselves strictly, but rather their habits are reconstructed after the fact, suggesting that this has more to do with generating probabilistic behavior patterns rather than conditions for discipline and control. Based on the line of thinking put forward by Haggerty and Ericson and

Whitson, they support the arguments presented earlier, in their contention that contemporary modes of probabilistic surveillance occur after the fact, gathering data to predict, rather than monitoring to coerce.

As Whitson notes, in the work of other surveillance scholars such as Ariane Ellerbrok and Torin Monahan, new technologies present surveillance in "benign," and "user-friendly" (Ibid, p. 164) ways which make the process of being watched seem subservient to pleasure. While this has been suggested by both Brighenti and Cousineau, Whitson suggests that the surveillance which takes place in this context cannot be understood until the role of play has been unpacked and inserted into the narrative of surveillant entertainment. Drawing on the work of Erving Goffman (1961, p. 18), she suggests that games provide an encounter with either other players, or cultural representations and expectations, which turn the game into a social experience through which certain social habits are "obliged" from the player, but within the context of their own personal freedom (Ibid, p. 165). Based on Whitson's argument, it can be understood that she conceives of play in two important ways which factor into surveillance. First, Whitson implies that play is largely rooted in habit, with players being awarded for "acting in accordance with the rules" (Ibid, p. 165) suggesting that there is a powerful psychological connection between play and repeating or often perfecting certain behaviors which games reward. Second, despite this desire to conform to certain rules, Whitson notes that an essential part of play is the freedom to engage in the experience, rather than being forced into the experience through coercion.

Whitson's attribution of habits and freedom are integral in understanding why an individual might submit themselves to surveillance as a form of entertainment. However, it is important, as Whitson does, to understand how powerful habits are built using digital technologies. As she argues, digital technologies are capable of providing a variety of incentives to encourage

individuals to conform to the various rules established by a game, often while simultaneously masking how these rules operate in the code of a program: “digitization allows the game to be distributed to a much larger potential audience, as the work involved in interpreting and maintaining the rules (and thus the system of social order) is taken entirely out of the players’ hands, and is instead reliant on algorithms” (Ibid, p. 166). This passage explains not only why games are effective (by automating the process through which a player might learn to discipline their behaviors), but how digital games easily permeate the lives of individuals, by being downloaded rather than bought, sidestepping the logistical dynamics that physical media, and other forms of surveillance, are often bound to. Building from these invisible disciplining forces, Whitson suggests that these systems are further incentivized through “juicy feedback, such as animations of spinning coins, joyful beeping sounds, and flashing point meters [that] indicate the system’s intended use, thus channeling players’ behaviour in a relatively consistent manner” (Ibid, p. 166). Ultimately what Whitson describes is a system which attempts to incentive self-perpetuating submission to a series of procedures which elicit a feeling of success. From this it is easy to understand how systems of surveillance might be inserted into the framework of these algorithmic systems to ensure that data collection is tied to the internal processes.

Looking at how digital games might be applied within the everyday lives of individuals, Whitson demonstrates that these experiences are integrated into digital technologies as “playful frames”: the gamification of traditionally non-play activities (Ibid, p. 164). The reason that these experiences have become so pervasive is because playful frames reinforce a technological mythology in our culture: the “neoliberal governance projects that promise to make daily practices more fulfilling and fun. Enabled by increased levels of surveillance (self-monitoring and otherwise), these projects use incentivization and pleasure rather than risk and fear to shape desired behaviours” (Ibid, p. 167). This observation is significant, as it suggests that the

application of digital technologies to monitor one's behavior is part of a larger societal process, though which individuals are encouraged to refine their behaviors, rather than shape themselves because of force or terror. While it could be argued that the fear of failure to comply with the mythology of self-governance is itself a coercive force, Whitson's observation speaks to the texture of self-surveillant activities. Moreover, she suggests that care becomes integral, as an individual quickly begins to associate notions of themselves with the digital representations of self they encounter in these games, tying their own personal progress to their progress in a digital environment. This she describes as "a teleology of constant and continual improvement, driven by an unending stream of positive feedback" (Ibid, p. 169). Positioning Whitson with respect to Cousineau's concept of "embodied cultural capital" in games, it can be understood that the former explains the feedback process through which this form of cultural capital is accumulated, sometimes tangibly and oftentimes psychologically. As a result, gamification and the surveillance it is tied to can be powerful psycho-social forces, rooted in both habit and performance of visibility, which might drive a user not only to monitor themselves, but to submit to a surveillant gaze.

While scholars examining the relationship between entertainment and surveillance have looked at numerous examples and different forms of media, their findings are remarkably similar. As they argue, surveillance in entertainment is subversive, particularly as a tool of indoctrination. The unproblematized appearance of surveillance in various media eases tensions and the controversial nature of both monitoring and prediction. While Brighenti has demonstrated that it is possible for art to subvert the surveillant gaze, it should be noted that her examples do not represent a coherent movement, as the meaning, insinuations and location of street artworks and other installations are undoubtedly illusive to the general public. Developing this argument further based on Whitson's research would suggest that users aren't dulled to the

experience of pervasive, but they are in fact *seduced* to desire engagement with surveillance as a social benefit. At the same time, the domestication of the surveillance industry is also disconcerting, as it suggests movement not only towards further expansion of surveillance technologies by de-skilling its labor, but also intimates the greater ease with which surveillance technologies can manage and organize the data they collect. The consensus emerging from these scholarly analyses indicates that there is further research needed to understand the processes through which surveillance embeds itself in entertainment media, how these experiences can be understood as pleasurable, and to what extent these experiences are relevant and predicated on other movements within the culture of art, games and other media.

2.3 An Algorithmic History: Cultures of Surveillance and Videogames

The early history of videogames is lost to time: many of the earliest videogames which likely ran on military computers, programmed by scientists and technicians, were never documented; to their creators they were likely the byproduct of other programming projects. As Nick Dyer-Witheford and Greig de Peuter note in *Games of Empire* (2009), some of the earliest creators of games, who were part of the military industrial complex, were given "lots of latitude" as "fooling around with computers, was a least tolerated because that was the way to discover new uses" (Ibid, p. 8). This lack of a definitive origin for videogames is in some ways fortuitous in understanding the history of videogames, not as the creation of an individual scientist or programmer, but rather as a multitude of disparate sociotechnical narratives which have coalesced into the modern videogame. Instead of trying to understand the history of videogames as a singular artifact, it is useful to understand how multiple paths within computing and surveillance converged and to observe how these artifacts have at times shared technical and cultural history.

One of the earliest threads starts in Los Alamos, New Mexico during the Manhattan Project in World War II. The city built up around Los Alamos provides a rare opportunity to study a place built from the ground up as a surveillance society. Historians including Garry Wills (2010) have argued that the work done at Los Alamos to create the atomic bomb generated not only a new form of political power -- bomb power -- but also a culture of surveillance and security that indelibly permeated American politics and society (Wills, p. 23). The creation of a new isolated city was necessitated by the absolute secrecy sought by its political directors who wanted to prevent any information about the nascent American nuclear program from leaking to the enemy or to the public. The denizens of Los Alamos were subject to constant surveillance and security procedures. Elaborate cover stories were designed to distract and misdirect public attention away from Los Alamos, trends that would permeate the intersection between American political and scientific culture for decades to come (Wills, p. 8). To support the atomic program, "human computers," female technicians assisted by mechanical counting aids, acted as a unit to perform the algorithmic calculations necessary to unleash the thermonuclear capacity of the neutron (Kean, p. 92). It would be on the principles applied through human based computation that the mathematical problem-solving of nuclear arms and the art of simulation through electronic computing would be honed.

When the Los Alamos project was closed its brain trust spread to the trade winds of the American military industrial complex. Many of the researchers who had been relocated to New Mexico during the war found their homes in new labs, including New York's Brookhaven National Laboratory. Brookhaven was governed by the Atomic Energy Commission (AEC), the civilian offshoot of the American military's nuclear program, and while it was remarkable because many of America's brightest physicists worked its labs handling problems related to atomic and nuclear safety, the lab was also special because it served as one of the first places

where a videogame was developed and *documented* (Guins, 2014, p. 102). When public sentiment towards nuclear programs soured for fear of their destructive power and ecological impact, many residents of New York and New Jersey were outraged by the proximity of a place like Brookhaven to major metropolitan areas. In 1958 Brookhaven's administration reacted by holding an open house, where the public could see the operations of the lab and have their fears assuaged (Nowak, 2008). To this end, Tennis for Two, one of the earliest recorded videogames, was developed by William Higinbotham and Robert Dvorak as part of these public showings of Brookhaven's labs. Higinbotham believed that the open house would be boring and dry, and reused some computers and other electrical components from his lab to build the game (it was not programmed, as the computers were analog, not digital) in less than a fortnight, using his expertise in targeting atomic weapons from his time at Los Alamos (Guins, 96).

Tennis for Two, a simulated tennis game which ran on a Donner model 30 computer and a primitive monitor known as an oscilloscope, was swamped with visitors who lined up for the chance to both watch and play the game. Little did the public know that the workhorse of this videogame spectacle was a computer designed to predict the yield of nuclear arms, and to estimate payloads and trajectories. Built on military grade computers, Tennis for Two was adept at simulating trajectories. Higinbothan had merely turned this ability in on itself to mimic the parabolic trajectory of a tennis ball as it bounced from racket to racket (Nowak, 2008). Tennis for Two demonstrates two important traits of videogames: first, that the computing origins of videogames are closely intertwined with a military industrial complex dedicated to the actuarial management of its arms through simulated use. Indeed, the simulacra of action present in most modern videogame arises out of the ability of computers to perform beyond the capacity of a powerful calculator, to act as devices capable of rapidly resolving algorithms and represent their resolution as action or movement rather than a series of static calculations. Computer systems

capable of performing these kinds of recursive calculations did not emerge out of thin air; rather they were the product of a government and scientists involved in simulating their capacity to wage war.

The second trait of videogames, which is evident in Tennis for Two's exposition during Brookhaven's open house, is one related to spectacle. As previously mentioned, the public was enthralled with the early videogame and a second open house was held in 1959 where the game was again displayed. The exposition of Tennis for Two and the sensation surrounding the game belied some difficult questions, such as: why had a nuclear safety laboratory developed a tennis game? What did Tennis for Two tell the public about atomic safety? The fact that these questions were never asked in any substantive way in the late 1950s is indicative of the fact that the secrecy of America's nuclear program had been largely successful; what the American public was expected to glean from open houses at places like Brookhaven had less to do with the process and purpose of scientific research, and more to do with the *product* of scientific work. Civilians in the 1950s could not be expected to understand that analog computers such as those that built Tennis for Two were highly specialized devices that required a tremendous amount of both mathematical and electrical knowledge to build and maintain, the kind of expertise which at the time was only afforded to the American military and its subsidiary, the AEC. So while the Brookhaven institute barely resembled the Manhattan Project at Los Alamos, persistent traits related to secrecy, the misdirection of public attention and the use of computers for simulacra persist; in doing so, Brookhaven's administration was successful in directing public scrutiny away from its activities.

Ultimately the invention of Tennis for Two did not signify the dawn of the videogame industry; rather it was a glimmer of the possibilities presented by computing during its time. The

game's creators believed that the videogame was a novelty and went back to the 'serious' work of nuclear safety (Nowak, 2008). It wasn't until the 1970s and 1980s that the videogame would have a presence in the landscape of American popular culture with the arcade cabinet and early home videogame systems.

The arcades, recreation centers, and bowling alleys of the late 1970s and early 1980s served as the public gateway to videogames. Accordingly one of the affordances of videogaming in a public space was a performative culture related to their play: a good player might attract a crowd of spectators, or a challenger would 'quarter up,' placing a coin on the corner of an arcade cabinet to signify their desire to play next on the machine. Players not immediately known by their appearance would at least be known by their initials, which would be placed beside high scores that were repeatedly displayed at the end of a game, or while the game was in an inert state, attracting players with flashing lights and sounds. At their apex arcade games became a minor sensation in the United States with sponsored tournaments for the best players, proto-gamers vying for the top score on games like Asteroids and Centipede. However, the visibility of arcades was short lived: arcades were commonly seen as undesirable spaces for youth and the popularization of home videogame consoles caused the rapid decline of arcades in public spaces (Donovan, 2010, p. 307). With this shift into the home, videogames became a private endeavor for much of the 1980s and 1990s. During this time, games retained many of their arcade-like qualities: a player's score was often tallied and scoreboards were still used even if the systems themselves could not permanently store this information in their memory. In this way, the logic of visibility still permeated the games designed for home videogame systems, even if only in a fragmentary way.

When videogame systems began to connect to the internet, the public scoreboard and the visibility of playing games returned to the discourse of videogame culture. In 1999 Sega's videogame console Dreamcast pioneered internet connectivity and allowed users to vie for the top score not just among a small community of players, but with any user who could connect their system to the internet. Helping Sega to network its home videogame system was Microsoft, who provided the operating system for the console (Street, 2013 p. 12). When Sega's fortunes in videogame systems declined, Microsoft themselves entered the market with the original Xbox, which was fully networked for broadband gaming over the internet. For the second iteration of the Xbox, the 360, Microsoft heavily integrated the logic of performativity in videogames and the visibility of the arcades by implementing digital trophies known as "achievements" into the system-wide architecture of the device, known as the XNA framework.

This partial history of videogames has charted the deep ambivalence of computing in recent history. The videogame owes its origins to the military industrial complex's thirst for actuarial applications of computing in simulation. However, the games themselves represent a peacetime expression of play and leisure which has spawned a shared global culture around the videogame. However, the real commonalities between surveillance and videogames are evident in the computation of algorithms. In the case of the Xbox 360 these histories coalesce into tangible surveillant artifacts within games and the design of the videogame platform itself.

2.4 Conclusions: Towards a Surveillant Platform Study

This literature review and history have established the groundwork necessary to understand how Surveillance Studies can play a role in the analysis of a videogame system as a platform. First, it has established a coherent foundation of theoretical approaches to explain surveillance processes by analyzing the recent writings of scholars interested in Surveillance Studies. In doing

so, this literature review has established that surveillance is conceived of not only as a way of watching, but as a technique for governance through observation and risk management intended to optimize the exercise of power. Secondly this chapter has examined the work of scholars who have used Surveillance Studies as a critical approach to analyze entertainment and media. This analysis has emphasized how surveillance in media acts as a tool of indoctrination which is designed to inculcate users into and enjoying their own surveillance. Finally this chapter has provided a means of understanding how videogames and surveillance are comprised of interrelated socio-technical systems. It is vital now to shift focus and analyze the Xbox 360 itself to demonstrate how theories of surveillance can be used to frame the tracking that the platform performs.

Chapter 3

3 Achievements, Code and Software on the Xbox 360

'Triple A' titles are the videogame industry's equivalent of cinema's summer blockbusters. These games are replete with disaster scenes, multi-million dollar budgets and celebrity voices. Their release is often heralded by expensive marketing campaigns rivaling their film counterparts. Given the game industry's focus on production values and spectacle it might be surprising then that many players are often pulled from these immersive simulations by text notifications, a reminder that the games they are playing are being systematically surveilled by software running on their videogame platform of choice. These notifications represent the accumulation of virtual trophies -- what Microsoft calls "achievements", a system-wide platform of in-game surveillance pioneered on the Xbox 360 videogame console in 2005. Achievements act as recognition of a player's videogaming prowess and these trophies are facilitated by complex surveillant algorithms and code built into the architecture of contemporary videogames.

At first, the presence of overtly surveillant mechanisms in the playful game context might seem odd and unsettling. To explain the presence of surveillant mechanisms within the playful context of games, and specifically those found within the software of the Xbox 360, this chapter will first identify surveillant aspects of videogame code that facilitate data collection. This chapter will then analyze the methods of surveillance used by Microsoft in the software of the Xbox 360 to shape the way users interact with their videogame platform. In particular, this chapter will argue that Microsoft has obscured its methods for surveilling players under representational veneers related to the culture, design and technological spectacle of videogames, disguising the governing role of surveillance in using its platform. To support this argument this chapter will analyze various systems of surveillance present within the software and games of the

Xbox 360 which identifies users, mines their play for data, records their behavior, and ultimately discourages cheating and hacking to ensure the financial viability of Microsoft as a videogame console producer.

3.1 Surveillant Code, Ambivalent Politics

As the brief critical history in the last chapter demonstrated, the origins of videogames and the code used to write these programs has a distinct relationship to political systems of monitoring and control. However, it cannot be argued that all games, especially at the level of code, have an explicit political agenda. Rather, a certain amount of videogame code has always needed to track the player: in order to be interactive videogame code needs to be able to respond to input, represent the effect of this input, and provide complex forms of feedback. To this end, videogames have always required ambivalent surveillant elements, qualities which allow them to collect and react to input data, whether in the form of simple onscreen movement or in the calculation of complex algorithms used to generate the behaviors of non-player characters. However, it is important to understand that this kind of ambivalent code, the kind required for interactive play, can be modified easily to facilitate data mining and surveillance. Therefore, to understand how videogames and their code can be used to create a distinct gaze, like the one on the Xbox 360, it is important to understand how code common to most videogames can be understood to track the user.

First, it is worth considering how the tracking and monitoring functions of code can be thought of as ambivalent. In Surveillance Studies many scholars have sought to identify the ambivalent potential of surveillant practices. In his 1996 essay, *The Electric Eye in the Sky,* Gary Marx suggested that surveillance could be “a comical, playful, amusing, enjoyable practice” (quoted in Albrechtslund & Dubbeld, 216). Six years later David Lyon made similar remarks, observing

that surveillance is “Janus faced” calling attention to the duality of surveillance as a process which provides both potential benefit and harm to those subject to a particular gaze (Lyon, 2003, p.164). Both the arguments made by Lyon and in Marx, two of the earliest and most important surveillance scholars, runs contrary to many scholars taking up Foucault, who have associated the process of surveillance with an implicit form of harm. Similar arguments made by Haggerty and Murakami Wood, as noted in the previous chapter, associate surveillance with Deluezian concepts of governmentality and governance. By making these arguments Haggerty and Murakami Wood permit for the practice of surveillance to be understood as a potentially ambivalent process with its harm and benefit determined by context: the politics of a surveillant gaze and its objectives. A specific example of this kind of ambivalent gaze is Haggerty and Daniel Trottier’s investigation of the surveillance of nature, in which the pair describe the preponderance of technologies that exist for humans to track and therefore preserve wildlife, while simultaneously increasing mankind’s governance over the natural world (Haggerty & Trottier, 2013, p. 98). These arguments all acknowledge a distinct relationship between surveillance and its politics, while the latter in particular also suggests that as surveillant mechanisms increase, so do the structures that may be deployed to govern (and thus obtain power over) the subject of these gazes. To apply this kind of reasoning to videogames it is worth evaluating code to understand how their design can be understood to track and monitor operations. By applying this understanding it is possible to evaluate how a platform like the Xbox 360 can facilitate surveillance and in particular, facilitate a kind of surveillance which appears inconspicuous to videogame players.

In computer programming, there exist many techniques which are indicative of an ambivalent gaze. Methods including ‘observer pattern’ and modular ‘aspect oriented’ programming are intended to monitor interactions between the program and user, often altering the behavior of

code to suit observations made by the program. For the most part these techniques exist to resolve bugs or errors in a program, rather to perniciously monitor the user. Similarly, in the code of games there exist many functions and techniques used to track the user's input and their behaviors during play, facilitating the action of videogames.

The movement of data through code and its internal memory combined with user input from a device like a joystick serves as the technical process which makes the playing of digital games possible. Alexander Galloway argues that this process within games makes them "algorithmic machines" formed through a cybernetic relationship between "operator actions" and "machine actions" to create the "action" of play (Galloway, 2006, p. 5). Galloway's explanation notes that the play of a game derives from the way in which videogame code mediates the relationship between a player's actions (derived from an input device) and the computer's hardware through algorithms, storing data generated by the player and responding through hardware calculations (Galloway, p. 13). This explanation is minimal, but it is suitable for explaining the basic phenomena that occurs when videogames are played on a purely technical level. What can be interpolated from this description is that tracking mechanisms must exist to productively harness data being derived from an input device, indicating that there exist components of a computer program where this data is not only collected but used for certain computational purposes.

If we want to understand how videogames facilitate surveillance in a thorough way it is vital to understand that they are programs designed to operate like simulations. More specifically, videogames are simulations where an activity (real or imagined) is represented through the execution of code. The architecture of code is therefore important to the action of videogames, because as code is executed it is responsible for the flow of information to and from the user who is engaged with the simulation. For these transactions to occur, code must render information

passing from the user or the computer into a legible form which it uses to execute a series of instructions.

For example, the data created by the code when it receives input from a player through a joystick is shared among a host of processes. It could be translated into the movement of an avatar on the screen or used by the game's adversaries to hunt the player through a maze. It is here that the legibility of this information in code is integral to the mediation between user and computer. As Galloway has argued, videogame code "transubstantiate[s]" physical input into digital information. In turn, this translation of input into data causes physical activity within the computer: "at runtime code moves. Code effects physical change in a very literal sense. Logic gates open and close. Electrons flow. Display devices illuminate" (Ibid, p. 5). What is useful about Galloway's observations is that he explains how code facilitates a translation of physical and mechanical action into a single digital language. In effect, Galloway demonstrates that code mediates disparate systems, the physical input of the user and mechanical action that occurs within computer systems. What is intriguing about these processes of collection is that the surveillant aspects of code are ambivalent; they exist to ensure that videogames act as dynamic, seamless simulations where the role of computation is opaque, and instantaneous.

What is important about this transformative process is that at the level of code, both the user and the computer are, relatively speaking, talking in the same language. However, this language and its meaning is only known to the code of the game, as the user is instead provided with a representation of their input generated through the code, while the computer is provided with a means of computing this information through instructions provided by code. This implies that code is both opaque and asymmetrical: it exchanges information for the representational action that occurs within a game, that the connotations of which demonstrate that the actual application of a user's input and in turn, the effect that this input has on code and computer's execution of

code is obfuscated. By analyzing the design of code in contemporary videogames, we can better understand how this makes code into a surveillant process of informational collection.

To understand the role of videogame code as an intermediary and its potential surveillant applications, it is crucial to identity two common aspects related to their creation. First, complex computer programs use what are known as data structures, shared variables and internal memory. These are parts of a program where information is organized and stored to be shared between different parts of a program's code. To use a relatively simple example: the storage of information in internal memory is often encountered in a game's score, when a player's activities within a game are systematically monitored, tallied and displayed to represent the user's skill and success within a game. Each time the user performs an action designated by the game the score is retrieved from the internal memory of a program, updated to reflect this action, and then stored again within this structure. Various other functions can manipulate and change information in a program's internal memory, as it is specifically designed to efficiently store and share information throughout a program. Examples of this might include data stores that can be used in a static way to record things like a player's name or to create dynamic and complex algorithms which are shaped by the player's activity, like an artificially intelligent soldier whose behavior is derived from data and used to anticipate the player's tactics.

Secondly, videogames and sophisticated simulations frequently use discrete, modular code to simplify their design, breaking a program up into segments that perform various functions. These functions might include the computation of complex algorithms or the collection of input data from a joystick or videogame controller. These modular 'chunks' of code make it easier for programmers to fix and modify a complex program by editing specific operations as opposed to a large monolithic and incredibly complex program (Nutaro, 2011, p. 2-3). The modular design of programs also allows a programmer to reflexively use the function of these modules, recalling

them from code when needed to perform a specific task or to act in concert with other code segments. This storage and computation structure can produce complex results when manipulated by an algorithm, results that range from a ghost inexorably hunting a player through a maze in the 1982 arcade game *Ms. Pac-Man*, to the shape and size of waves swaying the player's pirate ship back-and-forth as it sails the rough seas of the Caribbean in Ubisoft's 2013 game *Assassin's Creed IV: Black Flag.*

While this explanation of how code is structured omits much of the complexity behind programming videogames, it usefully identifies significant components of these programs which are oriented toward surveillance. In particular, the explanation identifies two vital traits of videogame code. First, it reveals that these programs are structured around modules of code. Second it shows that there exist sites within this code where information is stored and shared for later use. The best model for describing this modular and discrete form of tracking found in the architecture of videogame code is what William Bogard has described as a surveillant "enclosure" which was described in chapter 2 (Bogard, p. 31). The design of videogame code bears distinct similarities with enclosures because the panoply of functional modules and the data structures act in concert, efficiently creating, capturing and sharing information. Among the traits of an enclosure is to ensure the "mobility" of information while simultaneously capturing its flow (Bogard, p. 5). This model is useful in understanding videogame code, because data is not arrested by the program but guided and shaped by the program into the representational action of games. Through this continuous process of information collection, code allows a computer to perform certain operations dynamically, mediating action and reaction seamlessly. This process is arguably responsible for the pleasure that comes from playing digital games, in their ability to provide automatic and meaningful representations of feedback.

In the videogame industry, the style of tracking performed by videogames is an important practice in the creation and marketing of games. As games scholar Alessandro Canossa writes in his essay *Reporting From the Snooping Trenches* the use of videogame code to track player behavior is referred to as "game telemetry" the "automatic collection of data [from games] over a distance, removing the necessity to have a human observer present during playtest sessions" (Canossa, 2014, p. 434). In particular Canossa notes the mobility of information collected by these systems, observing that game telemetrics is particularly effective because "it is now possible for developers to collect behavioral data from millions of players" (Ibid, p. 435), superseding older methods of data collection used to measure a player's enjoyment of a game, such as counting the number of quarters players used in a single session on arcade machines, studying their behavior in a lab or creating aggregate metrics constituted by of all the reviews of a game users have left online (Ibid, 433-434.) This positions Canossa's observations favorably with a conception of the tracking that occurs through videogame code as an enclosure, as users are increasingly being tracked without having to be confined to a lab or a single fixed space, free to generate flows of information independent of an observer. Thus the mobility of data generated by game telemetrics is far greater due to the quantity of data game developers are able to collect from these systems and because the data itself is far more natural as user behavior is taken from observations of their play during leisure rather than say, paid study in a lab.

3.2 Achievements and Surveillant Code

"Achievements," the digital trophies which Microsoft uses to reward players for accomplishing certain goals within a game, are a fascinating subject of study, as they represent the application of elements already present in videogame code to suit a deliberate agenda of monitoring and tracking through game telemetrics. Specifically, these digital trophies represent

the way in which Microsoft and the developers programming games for its platform have repurposed the pre-existing enclosures found in the code of games, and leveraged them to perform a specific process of surveillance. Analyzing how this tracking is performed on the Xbox 360 and how it is represented to the user is indicative of the way in which Microsoft has branded surveillant processes by appropriating videogame code and culture, disguising monitoring by turning the presence of surveillance into a game itself.

Achievements operate by leveraging the sophisticated software architecture of the Xbox 360 to communicate between different layers of software running on the platform at any given time. The first layer, the games themselves (and the code they run) communicates with a second layer known as a 'runtime environment', a kind of operating system called the XNA Framework which works in the background to share information between other layers of software. With respect to the collection of data, the XNA is an architecture designed to receive reports from certain in-game operations. When specific conditions set by a programmer are met, it receives an identifying "string" of data from the game, a sequence of bytes which is encoded with various pieces of useful information (Harbour, 2010, p. 127). The data contained within the string not only indicates that a certain condition of the code has been met, but also contains metadata including the current date and time and whether or not he Xbox was connected to the internet (Microsoft Developer Network, n.d.). In response, the XNA framework promptly attributes a digital trophy known as an "achievement" to the player and allocates a fixed amount of points known as "gamerscore" to the user's profile which serves as a quantified metric of their videogame success across all the games played on the platform. On screen the player is informed through a positive sounding "plink" noise, followed by small dialogue box appearing on screen, that the user "unlocked" an achievement. This process is illustrative of how the game not only

captures data, but how the XNA framework operates as the game telemetrics reporting system which collects data, attributes recognition to the user and passes this data along to Microsoft.

The process described in the previous paragraph relies on a network of software processes running on the platform to be able to provide this kind of monitoring and feedback. What might be surprising about this process of software operations is that it is relatively simple: a few small pieces of information are transmitted from the code of the game to the run-time environment and in an instant data is captured from play and stored (Harbor, p. 127). This structure is significant because it indicates that the console and its software perform little of this actual tracking; rather achievements rely on games themselves to have a tracking and reporting system built into their functions. Subsequently, the structure of this system, specifically its orientation towards tracking occurring within the games themselves, is illustrative of the pre-existing compatibility of digital games and systems of user data collection, as games are configured by their designers to constantly process and react to solicit further input, using pre-existing structures within code to perform the tracking. This understanding also lends itself well to Bogard's model of surveillant enclosures, eschewing a centralized panoptic model for a decentralized network of monitors: achievements are facilitated by a variety of much smaller, contingent and modular systems of tracking (Bogard, 1996, p. 77). From a programming perspective, this decentralized, modular model is beneficial because it means that system resources are only used when needed, whereas a centralized and continuous tracking process would require separate program(s) to monitor a user as they play and would be a constant drain on system resources.

Examining this decentralized tracking and its productive capacity demonstrates how powerfully the system can monitor game operations. Due to the modularity of code achievements create a robust system of tracking, building on existing traits of videogame code which can ascertain the state of certain singular gameplay objectives, such as "rescue the princess" but they

are also capable of recording more complex non-linear player activities, such as “shoot 100 zombies in the head” or “fall 5000 feet” -- data and statistics that are tallied over dozens, and often hundreds of play sessions with a game. The tracking of these complex non-linear player activities is the result of instructions found within modules of code which systematically record the frequency with which they are executed within the game’s code and the outcome of their application. This information is then transmitted and stored to a value database, an enclosure of memory exigent to the actual playing of games where data about game play is systematically recorded. When certain conditions are met, the instructions governing this database trigger the transmission of a string to the XNA Framework.[iv] Additionally, because the Xbox 360 is networked, it also transmits this information to Microsoft through the console’s network connection where this information is stored on the user’s account.

In summation, the tracking of play that occurs on the Xbox 360 is represented to the user as an achievement, but is indicative of a pervasive form of data collection that operates from within the architecture of videogame code, which is then exported to a central game telemetrics reporting (the XNA Framework). This approach to tracking play within a videogame appropriates processes related to the modularity and memory necessary for the operation of scorekeeping and gameplay in games and associates them closely to a form of monitoring which provides a sort of performance evaluation which can be seen in the objectives set by achievements. Looking at the code running on the Xbox 360 it becomes clear that the XNA architecture harnesses the legible, productive and reflexive properties of code to produce numerous data points situated around play on the Xbox 360.

3.3 Data mining and Games

One of the most obvious applications of the achievement system is for data mining applications which collect aggregate information about player behavior on the Xbox 360. As previously noted, each game contains an already articulated system for monitoring activity in games, but this system can easily be adapted to collect metrics on user behavior. In Microsoft's policy document describing the Xbox Live Terms of Use, the company notes that it reserves the right to gather data related to "statistics", "game play" and even time spent within certain menus or watching advertisements on the console. Additionally Microsoft notes that it reserves the right to share this data with "affiliates, resellers, distributors, service providers, partners, and suppliers," indicating that data derived in this fashion is shared among a diverse group of interests who would profit from this data (Microsoft, 2013). As Emanuel Maiberg notes in *What Big Data Can't Teach us About Videogames* the collection of user metrics has become a standard practice in the videogame industry, which uses such figures to understand how players are interacting with their games (Maiberg, 2013). This 'big data' approach to the collection of player metrics would allow a company to know how users are progressing through their games, to observe player behaviors used in certain parts of the game and even to diagnose bugs or bottlenecks in a game which were not resolved before the game was released.

This approach to the collection of data derived from play on a videogame platform is indicative of how tracking such as the achievement system facilitates surveillance, as companies are able to justify their practices through policy documents like the aforementioned Xbox Live Terms of Use and to facilitate this collection through their platform's network connection, raising significant questions about the transparent disclosure of what kind of data is being collected. Given how opaque these metric collection systems are, Maiberg has argued these systems have become instrumentalized in the transactional style game design. In a blistering critique Maiberg attacks companies that collect user metrics from their games, noting that many of these

organizations use this data to manipulate users into small in-game commercial transactions (Maiberg, 2013). Similar observations have been made by Canossa, who notes that game telemetrics are often implemented by game developers interested in "improving monetization" of their games, by optimizing their design to elicit user purchases in-game (Canossa, p. 434). Maiberg's argument suggests that the kind of tracking is a surveillant project of governance, wherein data collected from the behavior of players is used to elicit a behavioral change in their consumption habits within games. Additionally, Maiberg notes that these efforts have a tendency to compromise game design, as developers who use these systems to facilitate transactions are increasingly creating games that use positive feedback and its denial to psychologically manipulate or entice users into paying money for granular parcels of enjoyment (Maiberg 2013).

This strategy for game development is common in the contemporary mobile games market, where games are often available to download for free: users who progress through these games are often enticed, if not often forced to make small in-game transactions for real money to continue playing the game. However, this practice is also common on home videogame systems like the Xbox 360 which feature "downloadable content," or "DLC", small packets of game content which a user must pay for. Often this content is repeatedly featured in the game, making it seem as if the game is incomplete unless the user purchases the content, or players are left at a competitive disadvantage in networked, multi-player games (Sinclair, 2013).

Both Maiberg and Whitson have separately argued that aggregate collection of data in games is increasingly having deleterious influence on game design, with videogame studios opting towards data-driven game design processes and eschewing the expert knowledge of designers and the preferences of large audiences of players who represent the core audience of a specific game (Sinclair 2013). The result, as Maiberg argues, are vacuous games "reduced to a science,"

suggesting that games designed by data driven processes are transactions where enjoyment is the product of a financial exchange between the player and the game that metes out pleasure for money. In this respect it may be more appropriate to suggest that Maiberg's criticism of surveillance found in games reduces them to a crude business, a Pavlovian mechanism designed and honed by aggregate surveillance to extract a proportional value from consumers in exchange for pleasure by determining when they are most engaged with a game, limiting the artistic expression of game designers, the enjoyment of players and engaging in questionable business practices related to the manipulation of customers.

This focus on data driven design has not only affected players who consume games as media, but also videogame designers. In an article summarizing a speech Jennifer Whitson gave to the Montreal International Game Summit journalist Brendan Sinclair noted that Whitson was particularly critical of the influence big data had on the precarity of jobs in videogame development, as game design companies seek to leverage data gleaned from games to further thin razor sharp margins between success and failure as a means of maximizing the profit from games produced with minimal labor and thus stifling new and innovative forms of game design. This argument reinforces those made by Maiberg questioning the artistry of games made through the analysis of user data. Whitson questions the ethics of game design companies which invest heavily in metrics, rather than design, arguing that such decisions harm both game developers through the allocation of financial resources (and the costs associated with analyzing metrics) and those of videogame players who find themselves increasingly at the mercy of developers pandering to sudden movements and shifts in their metrics (Sinclair, 2013). The criticism tabled by Whitson further reinforces the disparity between those who control the platform of game design and those who design and consume games. As these criticisms suggest, the artistic and even pleasurable elements of games are often at the mercy of large institutions that make

technocratic decisions based on data rather than expertise or consideration of the designer or end user. In addressing applications like data mining, it becomes evident that the collection of user data isn't an innocuous process on the Xbox 360, but rather a project of surveillance intended to reflexively shape the way games are designed and the way in which their audience consumes this media through risk management and manipulation.

3.4 Opaque Videogame Platforms: the Limitations of Blackboxing

Primarily this chapter has utilized a methodology which has analyzed existing techniques for coding games and specific documentation related to the way games on the Xbox 360 are coded. While this approach has yielded some useful information, videogame systems like the Xbox 360 are often defined by their lack of transparency: one of the trade secrets of videogame platforms is how their proprietary systems operate. In effect videogame consoles are "black boxes": devices whose detailed operations are only known to their producers. This makes investigating a device like the Xbox 360 challenging because analyzing a specific element like software based on its output to the user only provides some of the details regarding its tracking capabilities.

Due to this lack of transparency, it is worthwhile to analyze artifacts exigent of the device's electronic components to identify surveillant aspects of the Xbox 360's software. Policy documents like the Xbox Live Terms of Use provide another way to identify the operations of the system as this document identifies many of the privileges Microsoft reserves when a user operates their videogame platform. Among other demands, Microsoft notes that it reserves the right to "track, store, copy, distribute, broadcast, transmit, publicly display and perform, and reproduce: (i) your game scores; (ii) your game play sessions" (Microsoft 2014). In effect, this document acknowledges that the Xbox 360 possesses invasive surveillance processes capable of directly recording a user's game play that are not documented in much technical literature

provided to game developers. These kinds of acknowledgements, buried deep within policy documents, demonstrate a troubling aspect of networked videogame systems, in their ability to unilaterally monitor users with relative impunity. It raises significant questions about the privacy of users with respect to the political economy of videogame system production.

3.5 Conclusions about Software and Data on the Xbox 360

While this chapter initially focused on the latent aspects of code and videogame culture which could be construed as conducive to surveillance, the key shift demonstrated a transition away from ambivalent processes of surveillance towards those branded and governed by corporate interests, in this case mainly Microsoft's. The consequences of these monitoring systems within the videogames industry and culture are widespread, influencing the design of games, the pleasure to be had from playing them and even the personal privacy of users who play games with these tracking systems built into their code. However, perhaps the most telling sign that these systems within videogames are surveillant is how inescapable they have become, indicating a significant power disparity between players and the peddlers of their entertainment.

This chapter has performed a very narrow series of tasks given how many different systems of tracking exist on the Xbox 360. First, it identified the features of videogame code that can facilitate data collection and secondly, it examined how those features have been modified and used on Microsoft's videogame platform. Finally, this chapter has furnished a consideration of the immediate applications of this software in data mining, mapping user behavior and straightforward surveillance of play on the videogame platform. In doing so, the main objective here is to establish the power and potential of surveillant elements on the Xbox 360. The following chapters will articulate the politics of this system, explaining how these systems are used by Microsoft to govern users and manage risk.

Chapter 4

4 Governing the Gamer: Identification, Marketing and Risk Management

Videogame platforms are a novel environment for understanding contemporary consumer surveillance applications due to the way in which they blur the performance of playing games and the identity derived from this activity with proprietary networks and identification systems. These identification systems and networks facilitate the operation of videogame platforms which combine a panoply of functions: turning computers designed to play games into multimedia systems not only wired to play songs, films and browse the internet, but also to access entertainment networks, digital marketplaces and increasingly, social media exclusive to specific platforms. To access all of this content on Microsoft's videogame systems users must register an account with Microsoft known as an "Xbox Live profile," an identification system named after the Xbox 360's proprietary gateway to the internet, Xbox Live.

This chapter will explore how this profile transfigures passive data collection into a form of governance which Microsoft uses to police user behavior in ways suitable to its financial success. Specifically this chapter will provide various ways of understanding how Microsoft enrolls, profiles and governs users. First, it will consider the way in which Microsoft has sought to inoculate users from perceiving its identification system as invasive by analyzing the techniques Microsoft uses to enroll players with an Xbox Live profile. Second, this chapter will look at the way in which Microsoft uses profiles as risk management tools in the highly competitive marketplace of games, sharing information from user's profiles with partners including game developers/publishing companies, advertisers and game retailers. Finally this chapter will consider the way in which Microsoft uses its identification system to police users,

examining the tenuous relationship between the identity of gamers and an identification used to monitor the behavior of gamers.

4.1 Enrollment: Restriction and Access

In examining how the Xbox Live profile is used to govern players, it is worthwhile to consider how they are enrolled in this system and why they would be inclined to perceive the tracking elements that it constitutes as a positive feature, or even as a necessary tradeoff to play contemporary videogames. Many of the reasons a player might enroll in this system has to do with the way in which Microsoft has restricted the functionality of its videogame platform to necessitate the identification of users. While the last chapter provided details about how Microsoft's game telemetry works, this chapter will connect that system to numerous other tracking components of the platform, drastically expanding the scope through which in-game tracking can be perceived as a form of surveillance. As with achievements discussed in the previous chapter, what may appear to be a trivial form of monitoring is often indicative of a much larger networked project of governance on the Xbox 360. Therefore, it is important to consider how Microsoft coerces users into enrollment through its proprietary control over essential functions of its videogame platform and identify the purpose behind this tactic.

The process through which the Xbox 360 enrolls a user into its identification system begins when the user turns on their system for the first time. Each player who uses an Xbox 360 is assigned an Xbox profile: password protected account which serves as a mandatory form of authentication which a user must submit before playing games on the system. Upon initializing the system or commencing a videogame the player is required to sign into a profile or enroll for a profile if one does not exist. The reason behind this process is made more legible when the Xbox 360 is networked: when a player connects to the internet with their Xbox 360 they are forced to

create a unique username for their profile and provide contact information, the details of which become their Xbox Live profile. The Xbox Live profile is also associated with the metrics a player generates, cataloging the games they have played and acting as a repository for achievements they have unlocked and gamerscore points the users have received.

It should be noted that it is particularly difficult for users to evade or resist enrollment in an Xbox Live profile. While a user could generate individual identities for each play session with the device, this approach would not only be cumbersome but it would also prevent them from accessing the full functionality of the videogame console. An Xbox profile is required to access any portion of Microsoft's Xbox Live network, the only portal through which the device can connect to the internet. Additionally, a user cannot receive a warranty service, software updates, use Microsoft's digital marketplace, play online multi-player games or even receive technical support without an Xbox Live profile. This restriction of these basic elements of the device is indicative of Microsoft's efforts to ensure a user has no choice but to submit to identification and the subsequent tracking that their videogame console facilitates. In *Wired Shut* Tarleton Gillespie describes the effect of these systematic and technical limitations as "effective frustration", wherein the "possibility of acting" against these systems is "staged, made… invisible... or quietly rebuked" as to structurate the application of these devices in a manner determined to be suitable by their creators (Gillespie, 2009, 206). What Gillespie's argument indicates is that electronic devices and their limitations are designed to deliberately and subtly shape user experience. With the Xbox 360 we can understand that the device subtly manipulates the user into enrollment by withholding functionality. Once enrolled, the user is then profiled turned into Murkami Wood's "dividual" (Murakami Wood, p. 18) through profiling wherein demographic information can be gathered from contact details, including probable income, race and other juicy details (Badea et al, 2009). Being profiled, as the last chapter demonstrated, allows Microsoft to begin filling its

databases with information gleaned from game telemetrics, including the user's gaming proclivities and behaviors.

4.2 Gamification as Enrollment: Bait and Track

The system described in the last paragraph could be thought of as 'negative access,' a kind of coercion which encourages enrollment into an authentication system to access functions limited by the device. While this approach explains the subtle forms of socio-technical pressure at work in creating a systematic tracking system, it does not account for the reasons a user might be enticed to submit to identification and subsequent monitoring. As Michael Massimi, Khai Truong, David Dearman and Gillian Hayes have argued, recording activities which constitute surveillance can be understood as a "situated phenomena, highly contextualized and intertwined with not only the abstract beliefs of the individuals involved but also their conceptions of the specific places, spaces, and interactions of the moment"(Massimi, Truong, Dearman and Hayes 2010, p. 65). Chief among the attractive qualities of obtaining an Xbox Live profile are the attribution of achievements and persistent rewards system offered by gamerscores through the achievements game telemetry system. This game-like framework seemingly expands the playful borders of games to encompass playing all games on the platform, but it is also designed to function as an inconspicuous element of tracking, as the previous chapter demonstrated. One of the elements of this game telemetry system which deserves further consideration is the way it is intended to shape user behavior and control user interactions with the Xbox 360. Understanding how users are enticed by the achievement and gamerscore framework offers some insight into how users are inoculated against seeing this kind of tracking as pervasive and unwarranted.

It is vital to consider how the game telemetry system which is represented to the user as achievements are deployed as both a reward and tracking system. In *Surveillance and Capture*

Philip Agre identifies the way in which institutions establish tracking systems and explains why there might be appeal to enrolling into these systems. One development Agre identifies in the deployment of a tracking system is an analytic process which "generates a grammar of action", wherein "somebody studies an existing form of activity and identifies its fundamental units in terms of some ontology" (Ibid, p. 109) As Agre notes, digital systems are well suited to the creation of this kind of classification because "programming languages and systems analysis frequently supply basic ontologies (objects, variables, relations) upon which domain-specific ontologies can be built" (Ibid, p. 109). As the preceding examination of videogame code has demonstrated, much of the analysis necessary for Microsoft to build a domain-specific ontology from the activity of play was already structured in a meaningful way through the pre-existing condition of videogame code. What is important about the creation of this ontology is that it serves as a classification and organization scheme that identifies certain actors within code and allows them to be networked: data structures, clusters of modular code, and algorithms are turned into an enclosure which harnesses their productive capacity to generate data. Based on this understanding of videogames and the code of games that run on the Xbox 360, we can understand that the actors are already in place and networked into a useful ontology for tracking.

The next step in the deployment a tracking system is what Agre calls a process of "articulation," which he notes are the ways in which data "units can be strung together to form actual sensible stretches of activity" (Ibid, p. 110). Articulation can be understood as a sense-making activity, wherein data derived from monitoring processes is integrated into coherent pieces of information which describe some or of action or behavior. Game telemetry, the data tracking system built into the architecture of games, can be thought of as a form of articulation through the way in which it builds relationships between play, chunks of code and data. Additionally, the attribution of points from achievements serves as a kind of universal framework

across all games on the Xbox 360, articulating a relationship between all games on the platform regardless of differences in design or genre. For example, the gamerscore points framework provides a way to compare a user's performance in a hockey videogame to their success in a puzzle game, creating a normative frame of comparison despite the fact that both types of games are significantly different at the level of code and semiotic structures related to how success is represented in-game. In effect, the articulation that occurs with gamerscore serves to create a horizontal, comparative framework between each game, allowing users to make intelligible comparisons of user success in all game across the platform.

Perhaps the most important step in inoculating user perceptions against the notion that their behaviors are tracked is that the monitoring system must be explained in a desirable or useful way to the subjects creating data. This process, which Agre calls "imposition," is the establishment of tracking as a "normative force" within a system which entices subjects to submit to their own data collection (Ibid, p. 110). Branding tracking as achievements is integral to the imposition of a tracking system, because it closely associates tracking with the experience of playing a game, appropriating concepts like goals, points and score by transforming them into achievements, achievement points and gamerscore. Whitson has described this process as putting a "playful frame" around surveillance: a re-contextualization of surveillance as a playful experience (Whitson, p. 164). Subsequently, the imposition of achievements acts as a representational layer which camouflages the existence of tracking by blending it into the multifarious systems of feedback provided by digital games. The horizontal framework provided by achievement points and gamerscore adds to this playful frame, as these systems can be through a quantification of player skill, not unlike the arcades of the 1970s and 80s, wherein a game's scoreboard would call attention to the best players and their scores. Subsequently, the Xbox Profile becomes the new scoreboard of the networked home videogame console as each

player's individual gamerscore is displayed publicly for others to assess on what Microsoft calls the "gamercard", a profile summary available to other users through the Xbox Live network. Based on this close association between a metric for skill and their profile, it can be understood that Microsoft has sought to closely associate a user's gamerscore with their identity on the network.

It is also important to assess the immediate gratification associated with the tracking of play in videogames. Jennifer Whitson has described features like achievements and gamerscore as "juicy feedback", sounds and other indicators like points that act as structural tools that create positive reinforcement and encourage user engagement (Whitson, p. 166). Similarly, Ian Bogost has referred to similar gamic experiences as "partial reinforcement," what he describes as a form of "operant conditioning" that can explain how individuals enjoy and experience games through becoming attached to the rewards system within a game's structure (Bogost, p. 6). What is important with respect to surveillance about this kind of feedback is that it is intended to associate positive feelings already extant within game structures with a deliberate sense of being monitored across the entire platform. In harnessing the gamic quality of behavioral reinforcement Microsoft effectively masks the surveillance performed by representing it as a game. This style of representation can be thought of as a form of gamification: the imposition of game-like activities and rewards systems onto a non-game context.

4.3 Gamification as Surveillance: Playing Spy Games

Microsoft's competitors have been quick to follow the corporation's gamification of surveillance on the Xbox 360. Sony, Nintendo and Apple have since implemented achievement-like systems on their videogame platforms as well. Popular videogames *Battlefield 4* and *DOTA 2* even allow users to analyze the data derived from their play for further analysis. Further, many

fan-made websites give communities free access to this information as a tool to inform strategic players who apply this information in competitive play. On mobile phones, software platforms like Fuseboxx permit game developers the opportunity to analyze how users interact with their games in the aggregate. These widespread surveillant practices may seem unsettling to those who do not play videogames, but games scholar Mikael Jakobsson has observed through a series of ethnographies that videogame players find the concept of achievements and similar representational presentations of in-game surveillance highly rewarding and engaging (Jakobsson, 2011). In particular, Jakobsson's analysis demonstrates that the presence of surveillance in videogames has been well-received in gaming culture as this watchful gaze is perceived to enhance and modulate the pleasurable experience of play.

On its face, the identification of a user, the monitoring of a user's play, and the attribution of awards for certain accomplishments can be understood as a software enhancement designed to extract more pleasure from the activity of play. The gamerscore metric simply takes the abstract notion of scores and points from individual games and imposes that system onto the entire activity of playing games. Examining the effect of the achievement system in *Achievement Machine,* Mikael Jakobsson notes that the attribution of virtual trophies and allocation points in Microsoft's games has correlated with both critical and financial success in the videogame marketplace (Jakobsson, 2011). In addition Jakobsson observes a trend among critics and players to demand achievements as a mandatory software operation within all games, even in older titles re-issued by Microsoft which did not originally feature these mechanisms (Jakobsson, 2011). This observation speaks to Microsoft's success in deploying its game telemetry on the Xbox 360, as users do not protest the presence of these mechanisms, rather they bemoan their absence.

Quantifying the experience of playing with the Xbox 360 through the use of achievement as gamerscore makes the everyday act of playing games its own kind of game. Jakobsson argues that achievements turn the everyday experience of playing videogames on the Xbox 360 into a "massively multiplayer game" comparing the achievement framework to games where hundreds of users role-play, organize, compete and socialize in a persistent online environment (Jakobsson, 2011). The problem with this analogy is that while massively multiplayer online games (MMOs) are evocative of a large multi-player game framework, not unlike achievements, the two games have little in common. Jakobsson's comparison fails to differentiate between the two games despite their divergent structures, differences which are worth considering. For example, playing an MMO like World of Warcraft is optional, a choice a user can make when deciding how to spend their leisure time. Comparatively, participation in the achievement game is obligatory: users are forced to play the achievement game whenever the use the Xbox 360 platform because of the way Microsoft has imposed and deployed its game telemetrics system into the functions of the videogame system. Subsequently, Jakobsson's comparison is problematic because it implies that a user has a certain kind of agency over the achievement game that in reality does not exist.

In order to distinguish the achievement game from Jakobsson's comparison to Massively Multiplayer Online games, it is useful to consider how these games differ drastically in their meaning by analyzing their design. Game designer Eric Zimmerman has argued that the quality which distinguishes games from one another are the rules, which inform the way in which play is expressed – establishing the 'meaning' of specific games (Zimmerman, 2012). Much like the videogames themselves, the achievement game has its own rules and a style of play that emerges from playing within this frame. One of the rules of the achievement game is that players receive diminishing rewards from playing the same game. This can be understood in the allocation of

gamerscore points for each game: most games on the Xbox 360 are allocated a maximum of 1000 points with some games offering more or less points depending on the cost of the game (Jakobsson, 2011). Most of the achievements in a game are reserved for matters of routine play and can be obtained with a moderate amount of gameplay time, while other achievements require mastery and therefore a significant investment of a player's time, diminishing the possible rewards a player might collect over a fixed period. Subsequently, rooted in the structure of the achievement game are diminishing returns over time. Based on this structure it can be understood that playing the achievement meta-game does not encourage fidelity to a single game, but constant and continuous consumption of games to accrue the highest gamerscore score. Contrast this to the massively multiplayer online game, where positive feedback mechanisms are awarded to players who linger within its structure, who play inside the game with temporal consistency collecting in-game currency, joining persistent organizations called "guilds and making their characters more powerful. By comparison, the achievement game is not about being the best player or improving as a player, but encouraging an idealized behavior, constituted around all games, a sort of meta-game which favors the steady consumer of game media.

Jakobsson's comparison of the achievement framework to other videogames is problematic for a number of reasons. It is understandable that in his ethnography of user engagement with achievements, his desire is to identify and understand user enjoyment. In this respect, his comparison to familiar game structures is justifiable as users might enjoy two different games for similar reasons. However, the focus of this thesis is to demonstrate the way Microsoft's game telemetry system alters the experience of playing games. While achievements are indeed themselves a game played by all users connected or disconnected from the Xbox Live network, not unlike an MMO, for the most part these games are fragmented from the persistent semiotic,

temporal, technological and institutional structures common to games where hundreds of users play a single game simultaneously. Rather, the achievement game is rooted in the playing of all Xbox 360 games, but one also rooted in the temporality and space of play on the device. So while success in an MMO is reflected in a player's ability to master a single game's system within an online community, the achievement game reflects a user's ability to consume game media, so that they might receive a variety of achievements. The achievement game is not about persistent and direct co-operation and competition as in an MMO, but about *consuming games* through a framework established by Microsoft through a highly structured interaction with a proprietary platform, rather than a singular game itself.

Therefore, it is far more useful and meaningful in understanding the kind of play achievements are intended to evoke to think of the gamerscore assigned by Microsoft as a meta-game: a gamified structure which persists around all games played on the Xbox 360 platform. As per Whitson, we can understand that surveillant techniques like achievements expand the "frame" of play, encompassing the everyday experience of playing videogames to "evoke [a] behavior change" (Whitson, p. 164). As Whitson and Bogost have noted, games are a particularly effective medium to elicit a behavioral change because of the way rewards are structured into the experience in that they provide. Prior to the imposition of achievements and surveillant mechanisms, the act of consuming game media happened in isolated game spaces with limited continuity. Playing a game merely increased a player's cultural capital through their videogame literacy and perhaps skill. By contrast, the achievement meta-game is situated around the non-play activity of consuming a diverse library of games. Subsequently, the achievement meta-game is reliant upon financial capital or access to those with the money to purchase games. Subsequently, the rhetoric embedded in play surrounding the game space of the Xbox 360 focuses squarely on consumption to achieve success within the game's structure.

Microsoft's imposition of a gamified structure around the consumption of games is indicative of the politicization of its tracking. Specifically the achievement meta-game rewards players who shift their behavior towards the constant consumption of games. In this way it can be understood that the achievement meta-game is an attempt to elicit behavior change from players in a way which directly benefits Microsoft's financial interests, instrumentalizing consumption as participation in the game, with achievements and gamerscore as the reward.

4.4 Gamification as Governance: P(l)aying to Win

In addition to encouraging consumption, the tracking associated with achievements can also allow Microsoft to use game telemetry and the identification system to govern and even discipline users. By examining how Microsoft governs users with these tools we can understand how Microsoft uses the data it collects assertively, and we can also understand how Microsoft conceives of intended uses for its videogame platform. In establishing how the corporation has conceived of the "right" way to use the Xbox 360, we can better understand how its objectives and politics pervade the design of the videogame platform.

In 2008, Larry Hyrb, the director of the Xbox Live network, revealed on his blog that Microsoft had decided to crack down on users who had engaged in "gamesave tampering": the deliberate alteration of saved game files which allows users to accrue achievements and gamerscore points without having to perform the tasks specified by the hacked games (see footnote for a detail explanation of gamesave tampering).[v] Hyrb notes that these offenders were punished by having their gamerscore reset to zero (causing them to lose any achievement points and achievements) and that the users would have the epithet "cheater" permanently displayed on their account profile (Hyrb, 2008). While Hyrb does not provide details about the incidents that lead to this crackdown on users, Microsoft's prescience of this situation and its reaction is very

telling in regards to how it uses surveillance on its platform to govern users. It is likely that Microsoft used the data found in the game telemetry data transmitted to the XNA Framework and detected certain patterns emerging from this information which pertained to users "cheating" the achievement system by altering files. One of the ways this kind of detection could have been performed is through an analysis of the string data transmitted to the XNA framework. It should be noted that Microsoft also logs the time, date and status of the device's internet connection among the data transmitted to the XNA framework when an achievement is processed. Patterns emerging from this data could ostensibly reveal certain details regarding users who exploited certain security gaps in the achievement system, or used certain bugs within games to obtain achievements with ease by cheating the games themselves. It is even probable that Microsoft is capable of retrieving game telemetry data from specific devices in a way which the company hasn't publicly disclosed, but is alluded to in their Terms of Use policies, described in the third chapter. While Microsoft's methods to identify behaviors it identifies as cheating are intriguing, their reaction to this kind of behavior is also illustrative of how it governs users and its network.

It is worth considering the symbolic weight of Microsoft defining certain behaviors as cheating and labeling such users as a "cheater." In Mia Consalvo's *Cheating: Gaining Advantage in Videogames* (2009) the games scholar might categorize the tampering of a player's gamesave files as a type of behavior wherein outwardly the user appears to be playing by a set of rules, when in secret this individual is actually subtly transgressing these rules to gain power within a game: in this case, the achievement meta-game (Consalvo, p. 8). As Consalvo observes, cheating in digital games has persisted as an element of this form of entertainment since the late 1970s. Originally, cheats acted as hidden secrets added to games by developers who wanted to hide hidden messages in their games or make the game perform amusing functions incongruous with the rules of the game. As gaming communities developed through the 1980s and 90s cheats

persisted through paratexts like magazines, guides and books for "ideal" gamers, who dedicated their leisure time to videogames. Consalvo calls these users "power users" who seek what she refers to as "game capital": knowledge and expertise of a videogame (Consalvo, p. 22). Consalvo's observation of videogame players is prescient, because before Microsoft entered the videogame market, certain groups of users were already becoming identified and categorized by their consumption of media and their expert knowledge of game systems. It is interesting then that this understanding of a cheater, as an expert user, bears certain similarities in how Microsoft envisions the ideal user through the achievement framework: a user who obediently consumes games media. The tension arises here from the disruptive nature of the cheater on the Xbox 360, as they use their expert knowledge of game systems to exploit loopholes and security weaknesses within Microsoft's system. Resetting the user's gamerscore to zero is a curious part of this strategy as it highlights the incongruity between a user's *identity* and the *identification* within Microsoft's network, depriving the user of their gaming capital by altering their metrics. This tactic highlights the proprietary control of Microsoft over identities on its network by its policing through the alteration of their metrics (or even the threat of doing so).

The categorization of users as cheaters also establishes how Microsoft uses simulation as surveillance. Based on its ability to identify users and track their behaviors with its telemetry system Microsoft could have simply penalized cheaters by depriving them of their illicit achievements. Instead, the users had all of their achievement points taken away and their public profiles defamed with the word "cheater." As Bogard writes, this kind of warning strategy is effective because it disguises "an absence with a presence" indicating that this user is and continues to be subject to Microsoft's governing gaze without being under constant scrutiny (Bogard, 1996, p. 26). Instead, the user may be recognized through algorithms which Microsoft uses to check the validity of a user's achievements. Therefore the flag on the user's account

serves as both an indication and warning to other users that the "cheater" deserves to be the subject of scrutiny and ridicule for violating behavioral norms established by Microsoft. Visibility is key to their punishment as these accounts act as a warning to other users. Subsequently, this expression of data collection is intended to shape both the perception and behaviors of users to discourage them from manipulating their information. This is a process Agre calls "instrumentation": the naturalization of data collection practices wherein "participants… orient their activities towards capture machinery and its institutional consequences" (1994, p.110). Effectively cheater accounts serve as the instrumentation of data collection systems, representative of Microsoft's power, acting as scarecrows or signposts which warn other users that if they are in contravention of Microsoft's policies they too will be stripped of the data that constitutes their identity within the network, and labeled as cheaters.

Based on this understanding of a cheater, it is revealing to evaluate the reasons behind Microsoft's decision to discipline users and defend the integrity of its achievement system. Cheating the achievement framework within Microsoft's network is threatening to its videogame platform for two reasons. First, it disrupts the achievement meta-game by allowing users to bypass the behavioral reinforcement techniques designed to elicit game consumption. Potentially the disruption of this system also threatens to erode its value among users who, amidst cheaters, would see the points framework as meaningless if easily exploited. If such a thing were to be widely recognized by a gaming community, the allure of achievements as an indication of a metric would lose meaning and the system would no longer be representative of user skill.

The disruption of the achievement framework also threatens to distort Microsoft's ability to obtain reliable game telemetry from users. If users are tampering with gamesave files rather than

playing the games, Microsoft would be unable to use their data for game analytics because the tampered files would allow users to effectively sidestep the actual play of games and simply receive achievements and points without effort by loading up these tampered files and "tricking" the Xbox 360's game telemetry system into thinking the user had accomplished certain objectives without having to perform them. Potentially gamesave tampering could also skew the kind of information being returned from the telemetry systems on the Xbox 360, making it appear as if in aggregate more users were accomplishing difficult tasks and completing games they had not completed. Over time this could provide false trends in Microsoft's game analytics, potentially jeopardizing the validity of the data which is shared with Microsoft's partners. These partners include game developers, publishers and retailers. Retailers in particular use this kind of data as a risk management tool to produce new games, while game developers and publishers use this kind of data to project sales of new games (as outlined in Chapter 2). In effect, security holes in the achievement framework threaten to upset not only the validity of the Xbox 360's game telemetry, but also its application as a data driven financial risk-management tool.

While there are many other episodes within the history of the Xbox 360 that demonstrate Microsoft's capacity to surveil, govern and discipline users, the example of gamesave tampering is illustrative of the way in which Microsoft successfully exercises control within its network. The gamesave tampering incident indicates the way in which the company exercises discipline from its monitoring practices. Further, the tactics of censure established by Microsoft for punishing its cheaters highlights how control over these networks is often executed in ways which are sometimes incongruous with pre-existing cultural norms regarding players and gamers. Ultimately, Microsoft's actions against gamesave tampering reinforces the company's desire to protect the integrity of its informational collection practices, as these violations threaten the viability of Microsoft's investment in gamic behavioral reinforcement techniques as well as

the game analytics data used by Microsoft and its partners as a risk management tool in the sale of games.

4.5 Data mining and Marketing on a Telematic Console

Given how stringently Microsoft protects the integrity of the telemetric and analytics data it collects from its videogame console, it is worth considering why this data is so valuable. One of the most important features of the Xbox Live profile is that it allows Microsoft to perform tasks that were once labor and time intensive by profiling users and collecting their data in aggregate, giving the company the ability to utilize user data to make useful business decisions much more rapidly and with less overhead in expense. Additionally, Microsoft has integrated its identification system on the Xbox 360 into its properties outside of its videogame system, leveraging its horizontal reach across the software industry and providing the company with a wide-reaching ability to monitor and profile users. In addition to serving as a logon for internet services through the videogame console, the Xbox Live profile also acts as a login to Xbox.com, Microsoft's portal for information and services about the platform. Effectively, Microsoft has turned its users into a free labor collective using its console and online properties to transfigure users into focus groups, market researchers and playtesters. This approach to the collection of user data highlights the surveillant elements of Microsoft's data collection practices as the company is able to extract valuable labor from its users, largely without their cognizance.

In 2001 videogame production was already a highly competitive industry, and by the time Microsoft entered the home videogame marketplace many longstanding companies like Atari and Sega had already made and lost their fortunes in the manufacture of videogame platforms. Microsoft's approach to digital games is unique because of its strategy of risk management. In the years preceding the release of its first videogame platform the company had little experience

producing digital games. Excluding a few PC games released during the 1990s, the corporation's primary relationship to digital games was rooted in collecting information about users and their perceptions of videogames through a division of the company known as Microsoft Games User Research (Canossa, 2014, p. 433). Canossa suggests this division of the company was highly influential in the development of data collection practices, noting that after Microsoft Games Users Research (Microsoft GUR) was established in the late 1990s, many of its practices and databases "continue to be used to this day at Microsoft" (Ibid, p. 433). The influence of quantitative data collection is particularly evident at Microsoft through the way the company test games to ensure they are well received by users. In 2007 *Wired* magazine reported that Microsoft subsidiary Bungie had opened a lab where it studied roughly 600 players in a lab environment to determine how they played, enjoyed and challenged the design of their forthcoming game, *Halo 3* (Thompson, 2007). Using data derived from interviews, observation of players and data pulled from the game, Bungie sought to tweak and refine their game. In one particular instance Bungie used data generated from a "heat map," a digital topography of playspace which tracks frequent areas where users would die or kill other players to learn that certain players were using terrain to create an unfair advantage in multi-player games (Thompson, 2007). Using the data collected from the lab Bungie re-designed the playspace in question to ensure that no player would be able to exploit this shortcoming of its design and ruin the experience of playing for others (Thompson, 2007). The application of surveillance here indicates that one of the focal elements of Microsoft's research-oriented approach is the application of user observation as a risk-management tool to ensure the success of forthcoming videogame titles.

Despite Microsoft's novel techniques for approaching game design from data collection in a laboratory, this is still a fairly traditional method for collecting user data to configure a game. More recently Microsoft has announced that it intends to fluidly modify and tweak games by

keeping specific parts of a game's code in cloud storage, allowing it to change certain elements of the game on the fly, without notifying the user (Pitcher, 2013). What Microsoft does not indicate is how it makes these decisions, which is undoubtedly through game telemetrics generated by users which can indicate faults in game design, further allowing Microsoft to rectify problems or imbalances instantaneously by examining the data generated from large swathes of users playing their games. This is not an uncommon strategy in the videogame industry, which routinely issues "patches" for games: small fixes that are installed to upgrade or tweak a game to ensure that users cannot enjoy unplanned advantages in a game by exploiting faults in a particular game's design. What is novel about Microsoft's approach is the way the company has streamlined this process. This swift process allows the company to sidestep longstanding components of the development such as traditional play testing, wherein employees and expert users are paid to seek out software bugs and errors in game design. This application of game telemetrics allows Microsoft to utilize its surveillance rapidly to alter its games and to create labor from play, effectively conscripting players as play testers who provide useful data to Microsoft in aggregate.

The role of user data in market research also plays a significant role in the ways that Microsoft uses surveillant elements of its user profiles. By 2001 Microsoft had already integrated data mining into the Xbox.com, contracting the company Digimine, a data mining firm run by Microsoft employees, to track users and their behavior as they shifted between their videogame consoles and personal computers. Using a database from its website Xbox.com and Xbox Life profile information, Microsoft and Digimine analyzed and compared the behavior of users, sending specific users targeted e-mails and offers regarding videogames that they had determined the user was interested in (Grimes, 2003). Later Microsoft and Digimine began sharing their information with videogame retailers, allowing Microsoft to demonstrate the efficacy through

which it was able to generate sales through targeted advertisements to retailers (Ibid). This strategy is effective for obvious reasons, as it encourages retailers to stock Xbox games based on the performance of targeted ads on Microsoft's videogame platform, but it is also effective for the subtlety through which Microsoft uses its data collection practices to turn users into market researchers by tracking their behavior.

While applications of surveillance for market research and play testing are useful applications of data collection regarding the sale of games, Microsoft also uses tracking systems to maintain civility among users playing multi-player games through its videogame platform. Offensive behavior in multi-player games is not uncommon: players frequently use racist, homophobic or abusive language to discourage competitors, while other players might participate in "trolling" wherein a user deliberately attempts to exploit elements of a game's design to ensure that fellow players cannot participate or enjoy their game. To ensure that players have positive experiences when playing online games through their videogame platforms Microsoft has often employed various systems to indicate the level of sportsmanship demonstrated by players.

Prior to the launch of the Xbox One, Microsoft's successor platform to the Xbox 360, Microsoft announced that it would be devising "community-powered reputation system" for online multiplayer games (Microsoft, 2013). The system which Microsoft describes is crowd-sourced and uses the opinions of other players to determine the standing of users who are ranked based on positive or negative interactions with other uses. This crowd-sourced reputation system is especially useful to Microsoft in matchmaking, wherein users are paired with one another in online multi-player games. To this end, Microsoft's matchmaking service uses an algorithm to rank the probability through which players with a good reputation will play together in order to reduce the probability that a good player will be matched with a poorly ranked player (Microsoft,

2013). In effect, this approach to reputation allows Microsoft to draft users into the role of online community managers, who monitor, rate and exclude abusive players from their online community.

Microsoft's approach to multi-player matchmaking through a crowd-sourced reputation system is simply another variation on the theme of using data generated by users to inform the way in which it governs its platform. Microsoft harnesses the visibility of users on their network and the user's desire to discourage abusive players in order to effectively police their online community. The process involved in this reputation system is undoubtedly effective, but also problematic. As Daniel Trottier argues, crowdsourced surveillance "exploits" the labor of those involved through a "rhetoric that celebrates and extols the virtues of this configuration" (Trottier, 2013, p. 15). This exact kind of rhetoric is at work in the press release issued by Microsoft which states: "at the end of the day, our goal is to match you with other gamers you'll enjoy, and create the best gaming community online" (Microsoft, 2013). What this statement fails to underscore is that users are the ones responsible for creating this community and that the real beneficiary of this system is Microsoft, as it ensures that players are not discouraged from paying an annual subscription fee to access premium online services.

Trottier's argument that Microsoft exploits free labor is also evocative of many of the other surveillant processes examined in this chapter. From game analytics, to market research, and community management, Microsoft has established a data collection process on the Xbox 360 which monitors relative streams of information which the company then uses to refine and govern the experience of using the videogame platform. As Tiziana Terranova argues in *Free Labor: Producing Culture for the Digital Economy* this harnessing of user data blurs the "distinction between production and consumption" as users are both playing and creating

actionable data for Microsoft (Terranova, 2011, p. 34). What can be understood from this argument with respect to the Xbox 360, is that Microsoft has effectively capitalized on the way information flows across its system and affiliated networks, harnessing user behavior through participation to produce socially shaped, actionable information. Considering these kinds of participatory systems Soren Mork Petersen has argued that "the architecture of participation turns into an architecture of exploitation and enclosure, transforming users into commodities that can be sold on the market" (Petersen, 2008, p. 1). In evoking the concept of an enclosure Petersen's argument is apt, as he identifies the way in which Microsoft harnesses, rather than arrests, flows of user information. Further the commodification of users can be identified in the way in which Microsoft not only performs game analytics using its telemetric systems, but through the way in which Microsoft shares that data with 'trusted partners.' Petersen argues that the "commodification" of content created by users coupled with their lack of agency makes them into "losers" through this arrangement; despite shaping and producing for these systems, users are provided with little agency or ownership over the networks and systems through which they produce their data for (Petersen, 2008). This kind of losing relationship is best understood in the lack of privacy protections or options available for users to opt-out of the multi-faceted data collection systems at work on the Xbox 360, but is also evident in the policies and practices which govern the Xbox 360.

4.6 Conclusions: the Joys of Conscription

This chapter has provided a comprehensive examination of how data is generated on the Xbox 360: beginning with enrollment and profiling, then ending in the actionable application of user data through techniques like game analytics. In doing so, this chapter has sought to identify surveillant processes which use a variety of methods, from subtle discouragement and incentivization, to participatory systems which encourage users themselves to take part in

surveilling other users and policing their online communities. What has been revealing about this examination is the way in which Microsoft has conscripted users into channeling their play with the videogame platform into commoditized flows of information which the corporation in turn uses to both ensure the security and the integrity of its networks, and thus improve the sale of its games. The common surveillant aspect to these multifarious systems is the way in which Microsoft holds power over users, despite its reliance on the participatory generation of information. This discrepancy in the power of the console producer over its users is indicative of the surveillant political economy at work on the videogame platform: information is utilized asymmetrically from users who are in turn not granted ownership or determination of their data.

Focusing on the theme of asymmetricality, the next chapter will examine the design of the Xbox 360's hardware to identify surveillant elements present in its construction. In particular, this analysis of the videogame platform's hardware will build from the profiling discussed in this chapter and Microsoft's policies discussed in chapter 2 to identify the way in which the Xbox 360 uses hardware to enforce policy and copyright through physical intervention against the user.

Chapter 5

5 Console Hardware, the Kinect and Repair

While videogames are often culturally relegated to the status of toys, the contemporary videogame system is built like a fortress: hardened against attack with surveillance tools, electronic countermeasures, and sophisticated encryption systems. These are not the only weapons in a videogame platform producer's arsenal: Microsoft and its competitors have used their leverage over proprietary networks, digital marketplaces and access to launch expensive litigation in order to provide an additional layer of defense against hackers and software pirates who might challenge the integrity of their devices. Powerful technologies are also at work in peripherals like Microsoft's Kinect which uses an array of sophisticated sensors originally designed for military applications to "watch" the user for various purposes. As this chapter will argue, the technologies used in the Xbox 360 extend the console's surveillant agenda of securitization and risk management into the homes of users to the detriment of their personal privacy, eroding the rights of these users in the ownership of their devices.

In support of this argument the research performed in this chapter samples a variety of technical documents and resources written by computer hackers, security professionals, and security hardware vendors that have played a role in hacking or securing the Xbox 360. In doing so, this chapter collects, arranges, and presents a variety of previously fragmented information about Microsoft's videogame console which has never been collected or presented in a cohesive way for analysis. This chapter provides a way of understanding how these technologies provide a means of monitoring, control and governance through informational collection processes linked to the hardware of the original Xbox, the Xbox 360, and Microsoft Kinect. In essence, this chapter offers a way of reading the design of the Xbox 360 hardware as surveillant, considering

both the way in which its design collects information as well as how it is used as a governance tool.

5.1 Hacking the First Xbox

To understand why the Xbox 360 is such a heavily secured system, it is worth analyzing the history of its predecessor, the original Xbox. To do this it is important to step back to the late 1990s and early 2000s when Microsoft first announced the device so as to consider the political and economic climate at the time. In January 2001 Sega, a longtime videogame industry stalwart, announced that it would cease production of its latest videogame console, the Dreamcast, leaving the business of making videogame platforms entirely (BBC, 2001). Arguably this departure of a major player in the videogame industry left room for a new competitor like Microsoft who had teased the concept of releasing a videogame platform at numerous trade shows in 1999 and had assisted Sega in developing the online capacity of its last console (Microsoft, 2000). Shortly after Sega's announcement, the antitrust trial *United States v. Microsoft Corp* (253 F.3d 34, 2001) closed in February and despite the court finding against Microsoft, many critics agreed that the company still maintained a fierce dominance over the software industry (Jenkins & Bing, 2007, p. 15).[vi] This dominance had stoked antipathy among computer users and hackers, particularly those in the open source Linux community who saw Microsoft's grip on the market for operating systems as anti-competitive and undesirable (Eisenberg, 1999). Around the same time, software piracy in the videogame industry had exploded due to the ease through which pirates were able to copy games and subvert copy-protection mechanisms on platforms like the Sony Playstation and Sega's Dreamcast (Kirriemuir, 2009, p.237-238). Against this social and economic milieu Microsoft would release its first videogame console in November of 2001.

Both software piracy and the community of Linux hackers would pose a threat to the security of Microsoft's Xbox. In a 2005 a paper documenting the history of security gaps in Microsoft's first videogame console was released by German hacker Michael Steil. Steil identified three groups of users who worked to hack the Xbox: Linux enthusiasts, homebrew software designers and software pirates who sought to make illicit copies of games that would run on the device. Spearheading "the Linux Project" which successfully installed Linux onto the original Xbox in 2002, Steil noted that Microsoft's first videogame platform was a particularly juicy target for Linux hackers because the system was built mainly with "off-the-shelf" computer components and sold at a subsidized price by Microsoft, making it a particularly powerful but relatively inexpensive computer and a symbolic target (Steil, 2005, p. 1). What is provocative about Steil's analysis of the security system on the Xbox is the networked approach he takes to explain how hackers went about circumventing this system. This networked approach is evident in Steil's argument when he suggests that Microsoft failed to anticipate the synergy that might emerge from three different groups of hackers who worked towards circumventing the Xbox's security. This attribution on this part of Steil is novel, because unlike a conventional hacker who might see the circumvention of a security system as the personal triumph of their work, Steil argues that the hacking of the Xbox represents a fundamental failure on Microsoft's part to address the concerns of users who sought alternative uses for their system (Ibid, p. 9). To support this argument Steil noted that Microsoft's competitor Sony managed to stave off having the security measures of its Playstation 2 compromised much later into the device's lifecycle because it supported Linux early on and thus, escaped the attention of the Linux community and its hackers (Ibid, p. 2).[vii] Given how unlikely a reciprocal scenario between Microsoft and Linux hackers might have been, it can be understood that Steil's paper documenting the security flaws of the Xbox served as a kind of moralistic posturing on behalf of Linux users: Microsoft suffered the

consequences of acting as a monopolistic and unilateral giant against a diverse group of interests who banded together to overcome a common enemy.

Despite its failures, the Xbox did feature a relatively sophisticated security system. One of the main elements of the Xbox security system was a kind of memory encryption, through a system known as a "chain of trust," wherein important instructions necessary to run software were assigned an encrypted signature which was required for the device's hardware to execute instructions (Henson & Taylor, 2014, p. 53: 3). To subvert this system Steil and his associates sought to interrupt the chain of trust by altering the first link in the chain: hacking the read-only memory (ROM) chip responsible for the device's behavior when it is turned on. Using access to specialized tools at MIT, PhD student and hacker Andrew "Bunnie" Huang downloaded the data stored in this ROM chip and extracted the encryption key necessary to abrogate the device's encryption system entirely (Steil, p. 5). By subverting this encryption system hackers were able to run unauthorized code and install custom hardware onto the Xbox, allowing pirates, Linux hackers and homebrew software enthusiasts to have free reign over the device. Huang's investigation into the chip containing this information also yielded some fascinating data regarding the development of the device, including a penultimate version of the encryption system on the Xbox which was left on the device after production. Steil speculated that this data was accidentally left on the device in Microsoft's rush to bring the console to market shortly before the 2001 Christmas shopping season (Steil, p. 5). Other failures documented by Steil include poor selection of encryption algorithms by Microsoft engineers in designing certain components of the hardware. In particular Steil argues that Microsoft's security professionals, which later turned out to be interns, failed to note widely circulated critiques of the systems they used to encrypt data on the Xbox. The use of interns to implement and test encryption rather than seasoned security professionals was also raised as problematic and unprofessional (Steil, p. 13).

These failures to properly secure the system demonstrate that hardware security has less to do with powerful technology and rather more to do with correct implementation. Security is thus not exclusively a technological domain, but also a social and temporal relationship between designers, users and hardware.

Despite the diversity of problems which faced Microsoft once the Xbox's security was compromised by hackers, the corporation attempted to utilize a technocratic solution to resolve its problems. To fix security holes exploited by hackers Microsoft surreptitiously uploaded new software to Xboxes connected to the internet and patched their devices without first obtaining assent from the user to do so (Steil, p. 10). This incident is indicative of the kind of actions and behavior Microsoft is capable of in order to exert unilateral control over both its network and user hardware. While Microsoft's solution was easily overridden by hackers who found ways to 'downgrade' their systems and retroactively undo the patch released by Microsoft, it establishes the primarily technocratic means through which Microsoft has attempted to regulate its videogame platforms, which it continues to use on the Xbox 360.

Stepping back from Steil's partial analysis to consider the larger way in which the Xbox's security is situated, what becomes most telling about his observations is that they highlight the agency of a diverse array of human and non-human actors in securing a videogame console. In this respect, the security measures implemented on a device are not exclusively defined by what technological solutions are used to secure a technology like the Xbox, but also by socio-political factors like the Linux community's disdain for Microsoft, economic and/or temporal factors illustrated by the rush to get a device like the Xbox to the market before Christmas, and even the implementation of certain encryption algorithms in applications they are not suited for. Microsoft's reaction is also indicative of its failure to negotiate a network of actors, including its

own staffing shortcomings to resolve the security vulnerabilities of its device. Similar pitfalls have affected Microsoft's competitors like Sony, who in 2011 sued Playstation 3 hacker George Hotz for violations under the Digital Millennium Copyright Act (DMCA), the U.S. copyright law designed to protect intellectual property in digital mediums. In the aftermath of this litigation Sony faced an outpouring of cyberattacks, moral support from hacker collectives like Anonymous who saw prosecution against Hotz as a provocation to attack Sony's online videogame network and steal customer information (Kushner, 2012). In both cases Sony and Microsoft's simplistic response to a complex security situation only served to further undermine their desire to secure themselves against hackers by provoking their adversaries. Illustrative in these cases is that the security of proprietary hardware like the Xbox and the Playstation is of vital significance to their producers who are willing to go to elaborate lengths to defend the integrity of their videogame platforms.

5.2 Security and Surveillance on the Xbox 360

If the security on the Xbox was undone by a network of actors, the security on the Xbox 360 demonstrates how Microsoft has sought to develop a networked response to deal with the security of the Xbox 360. Using novel technologies, litigation, and control over access to its network Microsoft has utilized an array of techniques to oppose hackers and other users that might try to compromise the security of its next generation of videogame consoles. One of the most important elements of this networked approach to security are surveillant elements built into the Xbox 360's hardware which monitors the device's status.

A conceptually intriguing element of the Xbox 360's security is the device's hypervisor: a virtual environment where game code is executed and discretely analyzed to verify its authenticity. Like the original Xbox, the Xbox 360 uses the encryption technique known as a

‘chain of trust’ to ensure that the device’s hardware can only execute instructions which have been cryptographically signed by Microsoft. The hypervisor acts as an additional link in this chain because it serves as a filter which intercepts commands being executed by game software through a technique called virtualization. Virtualization occurs when software is tricked into thinking it is passing its instructions to the hardware: instead this program is communicating with another piece of software, the hypervisor, which mimics the function of hardware (Lees, 2005). Once the hypervisor intercepts these commands from the software this system inspects these instructions, ensuring that each line of code being executed is doing so in a way authorized by Microsoft. Provided that the code has been authenticated, the hypervisor sends encrypted commands to the hardware to process these instructions. After the hardware is finished executing its instructions it sends the new data back to the hypervisor in an encrypted format which is then passed back to the program which originally requested these instructions to be executed (Huang, 2007). This convoluted virtualization process prevents unauthorized instructions from being executed by the central processing unit (CPU) on the Xbox 360, while the encryption discourages hackers who might try to intercept data being passed to the device’s hardware from deciphering these instructions and using them to alter the hardware of the Xbox 360.

The security of the Xbox 360 provided by the hypervisor comes with a significant price for game designers developing games for the platform. The virtualization caused by the hypervisor is very selective about the instructions it will run, requiring a steep learning curve for software designers and creating a barrier for entry to amateur game programmers. In a 2007 presentation to Gamefest, a conference on videogame design at Rensselaer Polytechnic Institute, game designer and Microsoft employee Shawn Hargreaves noted that because of the hypervisor only a very limited set of instructions could be executed by the Xbox 360’s CPU. To compensate for this, Hargreaves suggests that independent game designers focus on executing a majority of

important sections of game code on the device's graphics processing unit (GPU) (Hargreaves, 2007, p. 15). Hargreave's suggestion indicates that independent game developers are likely restricted in their access to authentication from Microsoft and thus, excluded from using the full capacity of the platform they are writing programs for. Further, this distinction between game code being executed by the GPU, as opposed to the CPU, is significant particularly for independent game designers as it indicates that the system is so heavily secured so as to preclude significant design decisions because these users have limited access to important resources like the CPU. This observation is consistent with Gillespie's argument that the securitizing of technological design can significantly shape and marginalize expression: in this case defining how programmers design their games based on access to technological resources (Gillespie, 2009, p.8-10). What these observations regarding the hypervisor indicate is that Microsoft uses this tool not only to monitor and authenticate system operations, but to regulate game developers themselves: choosing who has access to what resources for developing games and in doing so, subtly shaping game design on their platform.

Another surveillant element of the Xbox 360 are known as eFuses, microchips which when given a specific signal are capable of dynamically reprogramming the way the chip processes data. Originally these chips were conceived to allow a computer system to perform self-repair by giving the system the capability to check if it was receiving the correct amount of power, and if necessary, allow a malfunctioning chip to reroute power in a way which resolves this issue and protects the computer it is housed in (IBM, 2004). However, on the Xbox 360 eFuses have a very different function: when a software update is installed on the Xbox 360 the device blows a set of eFuses and the chips report an encrypted value to the central processing unit (CPU). Using this encrypted data the CPU inspects all proposed software updates on the Xbox 360 and if it proposes to blow a previously consumed set of eFuses, the update is rejected. Effectively this

technology allows Microsoft to prevent the software on the Xbox 360 from being downgraded to a version with a security vulnerability which can be exploited by hackers (DeBusschere & McCambridge, 2012, p. 2). This technology allows Microsoft to effectively prevent the willful downgrading of systems by hackers who used a similar technique to circumvent Microsoft's security updates on the original Xbox. Positioning this technology with respect to Surveillance Studies scholarship, it can be understood that its effort to secure the device against forthcoming attacks is a realization of Elmer's argument that surveillance is designed to manage and govern the future, wherein the device continuously shaped and hardened by its producer prevents the user from exploiting past vulnerabilities (Elmer, p. 22). This singular application of eFuses is remarkable in that it *physically* restructures the way electronic signals are routed through the device in pursuit of specific governance applications related to the operation of the hardware. However, this technology also plays a significant role in tracking and monitoring the Xbox 360 and its user.

eFuses not only provides an additional layer of hardware security, but also acts as a surveillance tool. As a team of Linux hackers working on the Xbox 360 have discovered, eFuses are systematically blown in a specific way when an Xbox 360 is manufactured to give each videogame console a unique identifying signature (Free60, 2014). Subsequently, this kind of alteration means that at the level of hardware, each videogame console has a unique identifier which is reported to Microsoft when the device is taken online. This approach is particularly pervasive because it enrolls the device into tracking surreptitiously, without any obvious indication to the user that their device has a unique identifier. At the same time, this data can be joined with identifying information from a user's Xbox Live profile in order to create a link between the status of the device and users who have accessed their account from the device.

This form of unique device identification is significant because eFuses play an important role in allowing users to access Microsoft's online networks through the Xbox 360. As previously discussed in Chapter Four, the Xbox 360 can only access the internet through Microsoft's portal, Xbox Live; however if the system detects that the hardware of the device has been modified, a set of eFuses are blown to denote hardware tampering and this information is reported to Microsoft by the Xbox 360 when the device goes online. When Microsoft receives notification that this specific configuration of eFuses has been blown it uses this information to permanently prevent the device from connecting to its networks (DeBusschere & McCambridge, 2012, p. 2).[viii] This approach is particularly effective for a number of reasons. First, because the Xbox 360 stores critical system information in the chips themselves which are less vulnerable to attack and modification than the system's memory or storage medium (hard drive), it is incredibly difficult, even for a motivated hacker, to conceal this flag from Microsoft. Secondly, this approach allows Microsoft to reify its policy outlined in its Xbox Live Terms of Use, the end-user license agreement which Xbox 360 users must assent to which stipulates that a user must not "modify an Authorized Device [the videogame console] in any unauthorized way (e.g., through unauthorized repairs, unauthorized upgrades, or unauthorized downloads)" (Microsoft, 2013). This use of electronic countermeasures to enforce policy is highly problematic as Microsoft is engaged in legally dubious control over a user's property by overstepping the rights afforded to the user in owning the device. This behavior on the part of Microsoft is exemplary of Gillespie's argument that techno-regulatory solutions often allow powerful members of the culture industry like Microsoft to overstep the provisions of law in exercising control over their intellectual property (Gillespie, p.11). This outcome from the tracking supported by eFuses defines their surveillant application as tracking mechanisms used to instantiate a direct form of power over users.

eFuses and the hypervisor also play an important role in the simulation of surveillance due to their relative invisibility to the user and the effect they have in governing the system. Because these mechanisms are hidden from the user it creates the illusion that Microsoft exerts a totality of control over its videogame platform and that the corporation possesses a certain degree of omniscience over the operations of the device. This effort to both conceal surveillance and represent its totality is evident when a user's videogame console is banned from Xbox Live for hardware modifications. When the user connects to the network they receive a pop-up window on the screen which informs them that: "This console has been banned for violations of the Terms of Use. To protect the Xbox Live service and its members, Microsoft does not provide details about console bans. There is no recourse for Terms of Use violations" (Microsoft, n.d.) Screenshots and quotations of this notification appear far and wide on the internet, as many users who have tampered with the hardware and have been caught by Microsoft have sought recourse on the internet in both hacking and gaming communities. In this way, Microsoft's tactic with its ban notice is problematic for two reasons. Firstly, because it provides no technical details about why the console is banned, it leaves the user to surmise how they were detected. Secondly, the notice gives the user no recourse to appeal this decision, establishing that Microsoft is the sole authority on the legitimacy of the videogame console. In this way, the notification discourages users from challenging Microsoft's decision and considering hardware modifications given that they are unable to know if their modifications would be detected. Positioning this notice with respect to Surveillance Studies, Bogard has argued these kinds of notifications serve as the logical conclusion of surveillance, in that surveillant regimes would do away with actual "surveillor" and instead encourage the individual to police their own behavior, "saving the time and effort of policing him" (Bogard, p. 28). To this end, we can understand that the modification notice is effective primarily as a representational image of surveillance, a scare tactic, which

simulates Microsoft's omniscience of control over the Xbox 360. This strategy is effective because it precludes Microsoft from having to instantiate demonstrable control over the user, establishing that the company is always in control of its videogame platform.

5.3 Prosecuting Hardware Modification: USA v. Crippen

To secure and defend the integrity of the Xbox 360, Microsoft was also one of the first companies to support the U.S. government in taking a user to court for making unauthorized modifications to its videogame console. In 2009 Matthew Crippen was charged with two counts of having violated the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA) for modifying Xbox 360 systems to play pirated games. One particularly problematic issue for the defense in this case was that Judge Phillip Gutierrez ruled out a defense on the grounds that the modifications made by Crippen constituted fair use of the device. Citing the recently made provision in the DMCA that allowed for iPhones to be jailbroken, Crippen's defense attorney had hoped to have the defendant's Xbox modifications recognized in a similar way (Kravets, November 29, 2010). With respect to the modification of videogame consoles, the denial of fair use as a defense in court is incredibly important, because it contributes to the legitimacy of these devices as extensions of their producers, rather than the property of their owners. Ultimately, this kind of legitimacy allows the Xbox 360 to embody Haggerty and Ericson's conception of the surveillant assemblage: a convergence of actors (Microsoft, the users), technology (the videogame platform) and social systems (the courts) which reifies ubiquitous surveillance, legitimizing its gaze and making it inescapable (Haggerty & Ericson, p. 606). Subsequently, the judge's decision was not only important to Crippen's defense, but to establishing the authority of Microsoft to erode the ownership which users have over their devices.

Despite the judge's initial dismissal of a fair use defense, the case did not proceed in ways favorable to the prosecution. Much of the evidence heard demonstrates the effort that a powerful organization like Microsoft is willing to expend to ensure the prosecution of users who modify its hardware. Evidence presented in the case included hidden camera footage taken by a private investigator hired by the Entertainment Software Association (which Microsoft is a member) of Crippen modifying the consoles, and testimony from a Microsoft employee who had examined the consoles modified by the defendant (Kravets, December 1, 2010). However, these two key pieces of evidence were dismissed by the judge after he found that the hidden surveillance footage was submitted under false pretenses and that Microsoft's security expert had himself modified Xbox consoles during his time in college (Kravets, December 1, 2010). These pieces of evidence demonstrate an effort on behalf of Microsoft and its industry allies to reach beyond their technology and apply intense social pressure to users through a legalistic framework, adopting a networked approach to defend their hardware.

5.4 Surveillance and Repair: Obsolescence by Design

Often left out of discussions of hacking, fair use, and modification of videogame platforms, is the issue of repair when these devices break down. While videogame systems use increasingly sophisticated technology to produce dazzling effects, many of the technologies at work in these systems are both fragile and often precariously designed to be installed inside compact enclosures suitable for a user's living room. In the context of this chapter it is important to contrast the design of systems like the Xbox 360 which use proprietary technology capable of detecting modifications against the practice of repair, especially given the amount of troubling flaws which the videogame platform exhibits. One of the Xbox 360's primary design flaws was a tendency to overheat, causing the device's GPU's cooling system to disconnect from the

motherboard of the device. Unless repaired this flaw permanently disables the Xbox 360, preventing it from playing games, or even being turned on (Pullen, February 1, 2007). In a 2009 survey for the magazine *Game Informer* it was noted that roughly 54.2% of the Xbox 360's purchased by consumers failed, predominantly due to overheating or another technical problem (Eaton, August 19, 2009). Other surveys, like the one performed by online warranty company Square Trade, have provided a more conservative estimate: around 23.7% of Xbox 360 consoles have broken down due to technical problems (Thorsen, September 2, 2009). While this second figure is considerably lower, it is still a remarkably high failure rate for a commercial technology: if 23.7 percent of the roughly 25 million Xbox 360's sold in the United States have failed, this means that roughly six million of the devices were thrown away, sent to Microsoft for repair, or possibly repaired by users themselves (Alexander, March 11, 2011).

If an Xbox 360 falls out of warranty the user must decide whether to pay Microsoft for this service or attempt repair themselves. Users who decide to repair Microsoft's videogame platform must do so in spite of the device's design and mechanisms to discourage such an intervention. To repair a device, particularly a complex one like the Xbox 360, a user must learn not only how to diagnose the problem, but how to access the components necessary for repair. As infrastructure scholar Steve Jackson argues in *Rethinking Repair,* breakdown, like the failure of the Xbox 360 "occupies and constitutes aftermath… breakpoints and interstices of complex sociotechnical systems" which reveal the values embedded into our technologies (Jackson, 2013, p. 233). In this case, analyzing the breakdown of the Xbox 360 provides a way of revealing and evaluating its surveillant qualities and the politics at work in the design of the videogame console.

Jackson argues that repair is a "world disclosing" experience for a user, in that this kind of technological failure and reuse can expose the values instilled into a device through reflection on

how it has broken (Ibid p.230). It might be more apropos to say that there are worlds to be revealed by the failure and repair of an Xbox 360 -- the world and values of the Xbox repair communities online which stand in direct contrast to the world and values embedded in the design of the videogame platform. Professional repair and do-it-yourself repair solutions for the Xbox 360 have become a cottage industry on the internet. Websites like iFixit.com,[ix] a popular fixture of the D.I.Y. community, provide details on how to disassemble an Xbox 360 as well as many other contemporary videogame consoles. iFixit in particular operates like a collaborative gift economy much in the same way as Wikipedia, with users regularly uploading schematics and instructions on how to disassemble a variety of electronic devices. Along with these instructions to repair the Xbox 360, a user also needs to purchase a repair kit from a vendor over the internet, which includes proprietary tools needed to open the device, thermal paste to re-attach the processor and frequently, a securing clamp to replace a proprietary hardware inside the Xbox which holds the processor securely (Llama.com, n.d.). Half of the tools in this kit are designed to reach into discrete crevices on the exterior of Xbox 360 and open the device, to break down its seamless design and in doing so challenge its operation as a "black box" which the user is discouraged from peering into. This is consistent with Jackson's argument that the act of repair "addresses systems of visibility", which is in this case requires the user to make visible the closed systems inside the Xbox 360 (Ibid, p. 229). To this end, repairing the Xbox 360 can be thought of as a challenge to the values embedded in its design, and a chance to make visible the components and seams deliberately hidden from the user.

In opening the case the user encounters the first two counter-measures designed to discourage the user from tampering with the Xbox 360: a system of proprietary screws which require a special Torx screwdriver and secondly, a seal (a holographic sticker) emblazoned with the Microsoft logo, which once broken makes the console inadmissible for service from Microsoft

(iFixit, n.d.). Proprietary screws have become common in the electronics industry, and their application is primarily designed to discourage users from opening a device with common tools they might have at home. In this respect, the use of proprietary screwdrivers is intended to exclude amateurs from performing their own repairs, encouraging them to rely on warranties or to accept the obsolescence of their technologies. This is consistent with Jackson's argument that design decisions related to the repair and care of a technology can often foreclose user agency (Ibid, p. 231).

The sticker found on the inside of this case is referred to as the warranty seal by Microsoft: it straddles the two halves of the Xbox 360 case and is used to verify that internal components of the device have not been accessed by the user or another third party (Microsoft, n.d.).[x] Once the case of the device has been opened and the warranty seal broken the user has successfully precluded themselves from receiving technical support from Microsoft and they may proceed to repair their Xbox 360 with certain limitations. For example, if the DVD drive to the Xbox 360 has failed, a user cannot simply replace this drive with stock components. Rather, the user must install a drive identical to the one found in their Xbox 360 or trick device by altering the firmware of the DVD drive. If an exact copy is not used, the Xbox 360 triggers the eFuses used to signal hardware tampering and both the device and user are permanently flagged by Microsoft has having had attempted to perform an unauthorized hardware modification. Subsequently, a user must use exact replacement parts or escalate to hacking the device in order to perform this repair (iFixit, n.d.). What replacing the DVD drive and removing the Xbox 360's warranty seal demonstrate are the lengths to which Microsoft has sought to push the act of repairing its videogame console into illegitimacy, equating users who simply want to repair their device with pernicious software pirates.

As a repair-oriented analysis of the Xbox 360 has demonstrated, Microsoft has gone to elaborate lengths to establish itself as the sole authority of its videogame console. This strategy has meant alienating users who have been marginalized by significant material defects in the design of the videogame platform. However, these details on how to repair the Xbox 360 also reveal many of the implicit structures related to Microsoft's deployment of the device, in particular Microsoft's lack of product testing in its inability to predict such significant failure rates with respect to its videogame console.

5.5 The Kinect: Physical Rights Management

Invariably, any consideration of the Xbox 360's relationship to surveillance must address the device's camera/sensor peripheral, the Kinect. This is because more than any other component of the Xbox 360, the Kinect demonstrates how Microsoft has used the spectacle of advanced technology to contest the user's control over their property and apply surveillant techniques to instantiate controls over copyright and information far beyond the regulations established by copyright laws and reasonable expectations of privacy. It is also appropriate that the Kinect is the final component of this thesis analyzing the Xbox 360, because the sensor iterates on many other surveillant elements of the videogame platform including: the conscription of user data, hardware design intended to frustrate the user and the representational use of play to inoculate the user against perceiving the sensor as a tool of pervasive surveillance.

Introduced in 2010, Microsoft's Kinect is a powerful suite of sensors intended to allow users to use natural expressions like body movement and voice commands to interact with videogames. Marketing for the Kinect uses the phrase "you are the controller" to emphasize the way in which the Kinect could be used to enhance the simulation of activities represented in videogames by allowing the user to control games with "natural" gestures (Harper & Mentis,

2013, p 167). To this end, the Kinect contains a traditional digital camera sensor, an infrared (IR) projector and an IR sensitive camera which tracks the user's physical movement, while a microphone records audio input. The traditional digital camera senor records images using the visible light spectrum, while the IR camera and projector utilize a technique called "depth mapping", wherein the camera measures the time in which it takes infrared light to bounce off of an object and back to the sensor (Carmody, November 3, 2010). This technique in tandem with software running on the device which facilitates 'machine-learning,' allows the device to identify people using pre-set templates related to posture and pose: to categorize individuals and separate them from furniture and other non-human objects (MacCormick, nd.). These techniques empower the device to infer both 2D and 3D movement that occurs in front of it, making it an incredibly powerful device for tracking human gestures.

Despite the intriguing power of the Kinect, there are reasons to question and interrogate the way in which the technology purports to make interaction with videogames "natural." As Microsoft researchers Richard Harper and Helena Mentis (2013) have argued the language used in the marketing of the sensor is deliberately "evocative", of an idealized human-computer interaction, wherein the technological "barrier" to experiencing games –the controller— is removed from the equation. "So the hype goes, we are allowed to be natural. All other means of interacting with a computer are, by dint of this phrase, implied to be some-how other than natural" (Harper & Mentis, p. 167). Subsequently, Harper and Mentis question this line of reasoning, arguing that while gestures enjoy a semiotic familiarity, they do not necessarily preclude the use of a videogame controller.

In particular, the researchers note that despite the Kinect's power it is not nearly powerful enough to recognize all gestures effectively; as they observe, users who interact with the Kinect

must learn "what kinds of movements 'work' and which do not. Key to this is learning (or figuring out) how the machine 'sees' and adjusting human body movement" is key to interacting with the device. To this end they argue that users have to begin to shape their movements to suit the Kinect "to do its business" (Ibid, p. 168). What the researchers observe then is the fact that the Kinect still "sees" like a machine and in doing so abstracts their input like a machine, in a way which is really no different from a controller. Subsequently the pair argues that despite the hype and technology the Kinect has a "mocking gaze": one which pretends to comprehend, when in reality the sensor itself is shaping behavior. Harper and Mentis observe that more often than not, human subjects using the Kinect are forced to contort their body in bizarre, frequently comical ways to be recognized by the device (Ibid, p. 178). What's important about this argument is that it recognizes that the Kinect is still a controller, one which forces the user to stand in front of a camera rather than hold a controller. Ultimately these observations demonstrate that the Kinect is not a better way of interacting with videogames, but a visual way of playing with these simulations. In recognizing this, it is therefore important to assess the other functions of the Kinect to understand how it operates outside the context of digital games.

Other issues also persist in analyzing the design and function of the Kinect. Conspicuously absent from the design of the sensor is a lens cap, or shutter to disable visual recording and protect the image sensors when the device is not in use. Additionally, the device has no on/off switch to allow the device to be powered off when it is not needed. Instead if a user wishes to prevent the Kinect from potentially recording their behavior as they use their Xbox 360 the user must disconnect the device completely from the videogame console. This design is deliberate in that it is supposed to allow a user to turn on the videogame device without a remote control using voice commands. This trait of the Kinect's design operates much in the same way the device coerces a user into enrolling into a profile by leveraging deliberate design limitations to frustrate

alternative ways of using or controlling the device. This frustration reinforces a theme with the Kinect that surveillance is a necessary function of the device: it emphasizes the materiality of surveillance Microsoft has sought to implement in that the device challenges the user's ownership by preventing them from controlling its functionality. To borrow a concept from Heidegger: the Kinect is never inert and off, the surveillance and tracking it offers is always "ready-to-hand," in this way the Kinect totalizes surveillance by creating an almost permanent surveillant enclosure in the space in which it is housed (Heidegger, 1996, p.66). It is therefore no coincidence that Britain's GCHQ had proposed using the Kinect's microphone to spy on terrorism suspects (and undoubtedly anyone else caught up in dragnet style surveillance) as documents leaked by Edward Snowden have revealed (Kain, February 28, 2014). This interest in the Kinect by the GCHQ is demonstrative of how powerfully the device asserts surveillance into the homes of users, opening a channel of information flow that is never off -- just not in use. While these deliberate design oversights are revealing, they only begin to speak to Microsoft's intended application of the Kinect.

The Kinect was supposedly designed to usher in a new era of new interaction with videogames, but even before the device was launched information began to circulate in the press that Microsoft's interest in the sensor had begun to creep towards invasive objectives. In the same month the device was launched, Dennis Durkin, Microsoft's chief financial officer for the Xbox Division, gave a presentation to potential investors at a conference sponsored by BMO Capital Markets (Gallagher, November 12, 2010). In his presentation Durkin noted that the Kinect was going to become a key part of Microsoft's strategy of targeting advertisements towards users, by recording them as they play games. "How are they [the players] engaged with a sporting event? Are they standing up? Are they excited? Are they wearing Seahawks jerseys?" (Hollister, 2010). What is provocative about Durkin's statements is that his summary of the

marketing applications for the Kinect does more to identify its capacity of the device as a visual sensor that much of the technical documentation released about the device. Specifically, Durkin elaborates on the capacity of the Kinect to recognize and identify not only posture, but response to emotional stimuli like excitement and the Kinect's ability to perform image recognition (the identification of logos). In response to coverage of this event from the *Wall Street Journal* Microsoft issued a statement to the newspaper noting that "Xbox 360 and Xbox LIVE do not use any information captured by Kinect for advertising targeting purposes" (Gallagher, 2010). While this statement might have been accurate in 2010, it is clear that Microsoft was only performing damage control for what it had planned with the Kinect.

Despite Microsoft's damage control in 2010, by 2012 the corporation rolled out its "Nu-Ads" program, a series of commercials played on the Xbox 360 that track viewer behavior and upload this data to advertisers in real-time using the Kinect sensor. In a press release issued on June 14th, 2012 Microsoft noted that it had signed agreements with Samsung, Unilever and Toyota to serve interactive ads for these brands on the Xbox 360. In this document Microsoft notes that these advertisements will use the Kinect to allow users to respond and interact with these advertisements (Microsoft, June 14, 2010). While these advertisements are not targeted at the user based on observations made by the device, the press-release about Nu-Ads does not mention that the Kinect collects behavioral data about viewers as they watch the Nu-Ads through the Kinect by analyzing their posture to indicate their engagement with the ads and their emotional state through behavioral profiling (Sherman, August 8, 2011). This strategy by Microsoft to suggest that profiling is somehow different from invasive targeted advertisements is significant to the way in which Microsoft represents the surveillance performed by the Kinect.

As Bogard has argued profiling is a kind of simulated surveillant process, wherein the qualities of a subject are already known through preliminary investigation of the subject. Undoubtedly, Microsoft is already well aware of the demographics of Xbox 360 users. In this way, profiling supersedes the need to invasively monitor and track a subject. Instead as Bogard suggests, the profile allows Microsoft and its advertising partners to "efficiently and quickly" scan subjects of Nu-Ads to determine the content of their responses and thereby judge the efficacy of their ads. "What's important is how the profile is drawn and that it operates in accordance with the parameters around which it was designed", in doing so a profile "guarantees or serves up" an intended subject whose response is of value to the watcher (Bogard, 1996, 27-28). In this way, the ads themselves are already targeted and it is not the subjects who are valuable but the content of their response to the ad. This is evident in the language of Microsoft's press release regarding Nu-Ads which notes that "brands can get real-time feedback from audiences, making TV advertising actionable for the first time" (Microsoft, June 14, 2012). Thus what can be understood from Microsoft's profiling and deployment of Nu-ads is that the targeting does not occur instantaneously when the user is presented to the Kinect, instead the targeting occurs as the commercials are produced using the analytic data yielded by Nu-Ads to refine and hone advertising. Semantically Microsoft sidesteps the privacy issues raised by users and journalists regarding targeted advertising by ensuring that the process of targeting is one step removed from the immediate observations of the sensor and abstracted to the domain of behavioral profiling as opposed to the visual profiling of targeted ads suggested by Durkin. This approach bears distinct similarities to the way in which Microsoft uses game analytics with its partners to improve and refine the design of their games. In this way, Nu-Ads also use the same conscription of user data to exploit the emotional and physiological labor of Xbox 360 users.

Outside of advertising, patents filed by Microsoft also describe the way in which the company hopes to use the Kinect as a tool to enforce digital rights management (DRM) systems through media sold on the device. The patent in question allows Microsoft to check how many users are watching a particular piece of media and if necessary, switch the media off or charge the user an additional fee should the number of spectators violate a pre-set allowance (Plunkett, November 6, 2012). While this patent has yet to be implemented by Microsoft in any of its media offerings on the Xbox 360 or Xbox One, its implications reinforce Gillespie's argument that content providers frequently engage in the use of technologies which allow them to overstep regulations provided by copyright (Gillespie, p. 11). However, perhaps the more harrowing implication of this patent is that the gaze of the Kinect transcends digital surveillance, creating real material consequences for its gaze. By using the Kinect or another sensor to enforce DRM, the system actually becomes one of physical rights management (PRM) wherein policies set by an organization can not only be enforced in real time, but outside of the digital landscape in the homes of users with the device. In deploying this gaze, with direct material consequences into the home, Microsoft effectively turns the space around the Kinect into a hybrid environment -- one that is the user's private place of residence and a space which is governed by Microsoft's interests, as expressed though surveillant technology. Consequently, the imposition of a sensor like the Kinect has significant implications not only regarding the power Microsoft has over the platform, but the power Microsoft has in physically shaping the way a user consumes media.

What this analysis of the Kinect has demonstrated are the ways through which Microsoft uses representations of play and interaction as a veneer to obscure significant traits of the technology it deploys in users homes. From the deployment of Nu-Ads, to its patents which utilize the Kinect to enforce DRM systems physically, this analysis of the Kinect has proven the ways in

which Microsoft has sought to use visual data and flows of information to profit and govern users consuming media on the Xbox 360.

5.6 Conclusion: the Sovereign Territory of Microsoft

Summarizing all of the ways in which surveillance is enmeshed in the hardware of the Xbox 360 is challenging, simply because of the numerical quantity of different ways in which the hardware of the videogame platform has instantiated surveillant processes. Instead it is perhaps more tenable to signify the meaning behind this panoply of surveillant systems. For one, the surveillant elements of these technologies speak to Elmer's argument that surveillance allows for the constant exertion of power (Elmer, p. 23): this can be understood by the Xbox 360's ability to turn the user's home into a hybrid environment, one that is both simultaneously private and governed by Microsoft. The Kinect is exemplary of this exertion of power, because it is never "off" when not in use, but rather ready-at-hand, passively waiting for the moment when it is called into action.

Secondly, these systems participate in a direct shaping of the ways in which the user consumes media, which includes not only the games but the platform itself as a kind of media. This can be understood through the way in which the repair-oriented analysis of the Xbox 360 has demonstrated how the user is discouraged from interacting with the technology inside the device. Therefore securitization of the Xbox 360 demonstrates the power disparity of videogame console producers over users through the device's opaque construction, depriving and discouraging users from taking the maintenance and repair of their property into their own hands.

It is worth arguing that the Xbox 360 exudes a kind of sovereignty. This is to say that the device has been structured in such a way that despite the user's ownership of the videogame console, its functions, integrity, security and its purpose is not to be interfered with by the user.

Microsoft has even gone so far as to reify this sovereignty through policies and technologies which are designed not only to prohibit the user from violating the device's functionality, but have found ways to police the user against intervention. As *USA V. Crippen* demonstrated, there even exist laws which actively allow Microsoft to prosecute individuals who violate the integrity of its device and countermand its security. While this argument is hyperbolic, it speaks to a certain truth about the Xbox 360 and perhaps more generally the current state of consumer electronics. Devices like the Xbox 360, the policies which govern their use and laws protecting both ownership and copyright have been configured in such a way to create devices which hybridize ownership and corporate governance. Consequently, the status of these technologies gives them a certain prerogative to perform surveillance with impunity, while signifying the user's inability to intervene against such systems. Having investigated this system thoroughly, it is now worth returning to a holistic analysis of this technology -- central to a platform study -- to demonstrate how surveillance effects the expression of media on the Xbox 360 as a whole.

6 Conclusion: The Politics of the Surveillant Platform

Prior to the launch of the Xbox One, Microsoft's successor videogame platform to the Xbox 360, the company was engaged in a negative public relations battle over technical details regarding its newest videogame console. Originally Microsoft had announced that the Xbox One would require a constant internet connection for the device to function. While Microsoft eventually conceded to the demands of users and potential customers (Swider & Fitzsimmons, June 19, 2013), what is fascinating about this incident is that it may serve as the first indication that users have begun to push back against the constant pervasive surveillance present in Microsoft's videogame platforms. Further, the intended requirement that the Xbox One be connected to the internet is illustrative of the surveillant trends observed in this thesis. Forcing users to keep the videogame console connected to the internet would have allowed Microsoft to permanently secure a constant flow of information: to collect telemetric data and ostensibly, protect the device from hacking by requiring it to receive constant authorization from Microsoft to operate. To this extent, this thesis not only describes how the Xbox 360 functions, but it also describes a system of surveillance which is slowly growing through iteration. While in this particular instance Microsoft was thwarted from implementing even more extensive user monitoring, it is a surety that new surveillant systems and security features have been implemented in the successor to the Xbox 360. As such it is useful now to provide some conclusive statement on the operation of the Xbox 360 and summarize the findings of this thesis.

6.1 The Political Economy of the Surveillant Platform

In his 2010 paper *The Politics of 'Platforms'* Tarleton Gillespie argues that platforms exude a distinct discursive quality distinct from the media expressed through the platform itself; and while Gillespie primarily discussed participatory online platforms it is worth considering how the

Xbox 360 can be understood as a discursive platform (Gillespie, 2010, p. 3). To this end, Gillespie notes that platforms "institute a way of being" in that they "sanction and sanctify a particular state of things" (Ibid). Gillespie's argument connotes that the operation of a platform as an intermediary has a distinct impact on the way in which media is expressed through that platform and the way it is consumed, giving it a distinct political character and political qualities. Positioning this argument with respect to the Xbox 360 as a platform, it is clear that the systemic surveillance performed by the device is indicative of the political undercurrents palpable in its operations.

Primarily the politics of the Xbox 360 can be understood in the lack of agency a user can exercise in the flow of information from the system. For example, the user has no say in how the device collects telemetric data, and subsequently there is no option or toggle to disable the Xbox 360 from collecting the information generated from a user's play. This lack of control is further compounded by the fact that the user's play data is clearly marketed by Microsoft to its partner companies for application in game analytics as outlined in the Xbox Live Terms of Use (Microsoft, July 2014). This profitable practice by Microsoft is done without remuneration to the users who generate this data and as such their information is effectively conscripted into action by Microsoft.

Similarly the Xbox 360's prohibition against user agency can be identified in the design of the device's hardware. Given the seamless approach of the platform's design and its systems which forbid and prohibit repair it can be understood that the Xbox 360 is designed in such a way to only authorize the user to engage with the device through specific channels of operation, playing games or consuming media as opposed to exploring or tampering with the device's hardware. In this way, the Xbox 360 encourages a kind of passive engagement with its systems, one where the

user constantly makes themselves legible to the systems designed to monitor their behavior. Countermanding these systems, as for example with the users who tampered with their gamesaves files or Matthew Crippen's modification of console hardware, has been met with stern punishment from Microsoft ranging from public humiliation to litigation. These approaches suggest that the Xbox 360 is a particularly authoritarian device, despite its intended playful functions. This political quality observed from the way in which users interact with the device suggests that Microsoft has sought to deliberately alter the power dynamics in using its device to ensure that it maintains a totalizing grip over the device's functionality, a control which is both indicated and exercised through surveillance.

6.2 Surveillance and the Shaping of Digital Games & Play

One of the explicit objectives of this thesis was to answer the question: does surveillance shape the way videogames are experienced on the Xbox 360? As this thesis has explored the topic, it has become clear that it has shaped the user experience, but often in subtle and complex ways. Additionally surveillance alters not only the way players experience games, but also the way in which designers create games, indicating that the surveillance systems present on the Xbox 360 can cut both ways.

Achievements are perhaps the most symptomatic example of the way in which surveillance has changed contemporary videogame experiences for users. Achievements create a distinct sense of continuity across all games played on the Xbox 360 platform. These digital trophies and the points they grant (gamerscore) unite disparate game experiences across the entire platform: making a player's success in a puzzle game akin to their success in a flight simulation or a first person-shooter set in World War 2. This continuity, created through points and trophies is itself not explicitly surveillant, but it begins to construct a persistent narrative about a user which is

always visible through their Xbox Live profile. In this way, achievements and gamerscore points begin to shape the identities of users on Microsoft's online networks: by indulging in the gamified context of consuming game media on the Xbox 360 user's identities become subsumed by these systems. As is the case with many games, the player who can accrue the highest gamerscore is better at the achievement game than the user with less, as evidenced through the user's profile. In this way, visibility begins and the behavioral reinforcement of a points systems bleeds into the user's online identity, by gamifying a user's expertise in games. In the past, players used to accrue what Mia Consalvo calls "gaming capital" (Consalvo, p. 2) in fragmentary and disparate gaming experiences across a variety of platforms. Comparatively achievements structure the collection of gaming capital: providing users with a way of identifying their gaming abilities. As Jakobsson has observed, this has lead to a beneficial perception of achievements as a system which enhances games on the Xbox 360 platform, driving players to compete for the highest score in this gamified context (Jakobsson, 2012).

However, achievements also demonstrate numerous problematic traits. First and foremost, the gamified context built around the collection of achievement exhibits exploitative qualities through the way in which this system utilizes a reward system to behaviorally reinforce the continuous consumption of games on Microsoft's platform. Secondly, should a player step outside the rules established for the achievement game by Microsoft, to cheat in order to inflate their Gamerscore, Microsoft has few qualms about punishing and/or humiliating these users. As the gamesave tampering incident demonstrated, Microsoft is quite comfortable punishing "cheaters" and making them subjects of public humiliation by calling attention to these users through their online profiles (Hyrb, 2008). This incident, more than any other, emphasizes the fact that the online identities which users are encouraged to craft are not malleable, but part of the Xbox 360's online network, the property of Microsoft. In this way, the punishment of users

calls attention to the difference between their unique identification and the identification system which Microsoft uses to govern its users.

The achievement system is also one of the most significant ways the design of games is affected by surveillance: through the processing of game analytics. As Maiberg and Whitson's criticisms have demonstrated, popularity of data driven design can often exclude the insights of game designers and expert users like players in favor of game designs which optimize the monetization of games or alter their composition to appeal to the broadest audience possible. As a result, data driven design processes threaten the artistry and authenticity of game development by pushing game designers to make games that privilege success in the marketplace, rather than games which are suitable to the designer's intended expression.

Peripherals like the Kinect also play an important role in the way surveillance can shape game design. As Harper and Mentis have pointed out, the Kinect's implementation as a device which enhances the experience of playing games by removing barriers like controllers leaves much to be desired in its efficacy to capture gestural input (Harper & Mentis, p.168). To this extent both researchers suggest that the future of remote game operations through gestural interfaces is probably bleak (Harper & Mentis, p. 178). Rather, as this thesis has argued, the Kinect seems much better suited to act as a tool of pervasive surveillance in Microsoft's marketing arsenal despite the privacy concerns for users. This situation has the potential to be problematic for developers committed to making games that incorporate the Kinect who might face a decline in interest regarding their titles due to user recalcitrance to adopt the use of a Kinect given its privacy implications, particularly amidst the constant barrage of public relations disasters sustained by Microsoft in deploying the sensor.

As Microsoft employee Shawn Hargreave's presentation to students at Rensselaer Polytechnic demonstrated, game design on the Xbox 360 is also shaped by the securitization of the platform. In his talk Hargreaves encouraged amateur designers to work around the security of the device, offsetting the execution of code onto the less secure graphical processing unit (GPU) as opposed to the powerful, but heavily secured central processing unit (CPU) (Hargreaves, 2007). These kinds of limitations can have a significant impact on the design of games and the plans of their designers, who must optimize the way the platform that executes code can ensure that games run smoothly and use system resources efficiently. Due to the fact that games are a hybrid of a designer's ability to work within the medium and a computer's ability to execute code, limiting the access of game designers to system resources not only alters the way these users approach game design, but it also potentially hamstrings their work should their games exceed the capability of the limited system resources they have access to. The effect is not unlike forcing an oil painter to work with crayons, with distinct implications on the way in which game designers craft and construct their art.

These arguments demonstrate the way in which surveillance alters the way games are experienced on the Xbox 360 and in doing so, realizes the explicit objective of platform studies as defined by scholars like Gillespie, Bogost and Motfort. However, it is also important to recognize that the implicit objective of this thesis has always been to unmask and reveal surveillant processes built into Microsoft's videogame platform and in doing so, call attention to their socio-political qualities through the locus of Surveillance Studies. As this thesis has explored, the surveillant systems of the Xbox 360 demonstrate that there exist many elements of these systems which improve or increase user engagement, providing users with new and novel ways in which to enjoy videogames. However, this thesis has also demonstrated that surveillance has had an unmistakably deleterious effect on the expression of games running on the Xbox 360

platform: depriving users of agency, exerting questionable control over copyright, exploiting user consumption habits and even altering or limiting the way in which designers can make games for the platform. It is perhaps ironic then, that the negative qualities which stem from widespread surveillance on the Xbox 360 are those qualities which cannot be gauged by its systems, demonstrating that even all-encompassing surveillance enclosures like those on Microsoft's platform can have blind spots.

Works Cited

"Achievement Members." *Microsoft Developer Network*. N.p., n.d. 25 Aug. 2014. <http://msdn.microsoft.com/en-us/library/microsoft.xna.framework.gamerservices.achievement_members.aspx>.

Agre, Philip E. "Surveillance and Capture: Two Models of Privacy." *The Information Society* 10.2 (1994): 102-127.

Alexander, Leigh. "GameStop Details Europe, U.S. Installed Base For Consoles." *Gamasutra Article*. N.p., 31 Mar. 2011. 25 Aug. 2014. <http://www.gamasutra.com/view/news/33842/GameStop_Details_Europe_US_Installed_Base_For_Consoles.php>.

Badea, Alexandru, Ruxandra Badea, Constantin Bagu, and Christina Moise. "Customer profiling using GIS." *Annals of DAAAM & Proceedings* 2009 (2009): 567.

Bogard, William. *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. Cambridge: University of Cambridge Press, 1996.

Bogard, William. "Simulation and Panopticism." *Routledge Handbook of Surveillance Studies*. Oxon: Routledge, 2012. 31-45.

Bogost, Ian, and Nick Montfort. "Platform Studies, a book series published by MIT Press, Ian Bogost and Nick Montfort, series editors." *MIT Press*. N.p., n.d. 1 Sept. 2014. <http://platformstudies.com/>.

Brighenti, Andrea Mubi . "Artveillance: At the Crossroads of Art and Surveillance." *Surveillance & Society* 7.2 (2000): 175-200.

Canossa, Alessandro. "Reporting From the Snooping Trenches: Changes in Attitudes and Perceptions Towards Behavior Tracking in Digital Games." *Surveillance & Society* 12.3 (2014): 433-436.

Carmody, Tim. "How Motion Detection Works in Xbox Kinect | Gadget Lab | WIRED." *Wired.com*. Conde Nast Digital, 10 Nov. 2001. 1 Sept. 2014. <http://www.wired.com/2010/11/tonights-release-xbox-kinect-how-does-it-work/>.

Consalvo, Mia. *Cheating Gaining Advantage in Videogames*. Cambridge, Mass.: MIT Press, 2007.

Cousineau, Matthew J. "The Surveillant Simulation of War: Entertainment and Surveillance in the 21st Century." *Surveillance & Society* 8.4 (2011): 517-522.

Crossley, Rob. "Interview: Phil Harrison on Xbox One's core games charge - CVG US." *Computer and Videogames*. N.p., 21 Aug. 2013. 25 Aug. 2014. <http://www.computerandvideogames.com/425845/interviews/interview-phil-harrison-on-xbox-ones-core-games-charge/>.

DeBusschere, Eric, and Mike McCambridge. "Modern Game Console Exploitation." *CSc 566 2012: Research Presentations*. Arizona State University, 2 May 2012. 5 May 2014. <http://www.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic1-final/report.pdf>.

Orwell, George. *1984*. Harlow: Pearson Education, 2003.

Deleuze, Gilles. "Postscript on the Societies of Control." *October* 59.Winter (1992): 3-7.

Donovan, Tristan. *Replay: the History of Video Games*. East Sussex, England: Yellow Ant, 2010.

Drachen, Anders. "What is game telemetry?." *GameAnalytics*. N.p., 23 Aug. 2012. 1 Sept. 2014. <http://blog.gameanalytics.com/blog/what-is-game-telemetry.html>.

"Earnings Release FY13 Q4." *Microsoft Investor Relations*. N.p., n.d. 25 Aug. 2014. <http://www.microsoft.com/investor/EarningsAndFinancials/Earnings/Kpi/FY13/Q4/Detail.aspx>.

Eaton, Nick. "Survey: Xbox 360 failure rate is 54.2%." *The Microsoft Blog*. Seattle Post-Intelligencer, 18 Aug. 2014. 25 Aug. 2014. <http://blog.seattlepi.com/microsoft/2009/08/19/survey-xbox-360-failure-rate-is-54-2/>.

Eisenberg, Rebecca. "Linux users unite against Microsoft." *San Francisco Examiner*. N.p., 7 Feb. 1999. 25 Aug. 2014. <http://www.sfgate.com/business/article/Linux-users-unite-against-Microsoft-3097722.php>.

Elmer, Greg. "Panopticon - Discipline - Control." *Routledge Handbook of Surveillance Studies*. Oxon: Routledge, 2012. 21-53.

Fahey, Rob. "Could Microsoft sell off the Xbox?" *GamesIndustry.biz*. N.p., 28 Feb. 2014. 1 Sept. 2014. <http://www.gamesindustry.biz/articles/2014-02-28-could-microsoft-sell-off-the-xbox>.

"Final Judgment : U.S. v. Microsoft Corp.." *Justice.gov*. N.p., 12 Oct. 2002. 1 Sept. 2014. <http://www.justice.gov/atr/cases/f200400/200457.htm>.

Foucault, Michel. *Discipline and Punish: the Birth of the Prison*. New York: Pantheon Books, 1977.

"Fusesets." *Free60*. N.p., 7 Jan. 2014. 25 Aug. 2014. <http://free60.org/wiki/index.php?title=Fusesets>.

Galan, Walter. "Xbox 360 Lower Case Replacement." *iFixit*. N.p., n.d. 25 Aug. 2014. <https://www.ifixit.com/Guide/Xbox+360+Lower+Case+Replacement/3330#s16030>.

Gallagher, Dan. "Is Your Videogame Machine Watching You?x" *Digits*. *Wall Street Journal*, 11 Nov. 2010. 1 Sept. 2014. <http://blogs.wsj.com/digits/2010/11/11/is-your-videogame-machine-watching-you/>.

Galloway, Alexander R.. *Gaming: Essays on Algorithmic Culture*. Minneapolis: University of Minnesota Press, 2006.

Gera, Emily. “Can your next-gen console spy on you?.” *Polygon*. N.p., 5 Nov. 2013. 25 Aug. 2014. <http://www.polygon.com/2013/11/5/5054400/can-your-xbox-one-spy-on-you>.

Gilbert, Ben. “The Xbox One price drop isn't just to boost sales, says Microsoft.” *Engadget*. N.p., 26 May 2014. 25 Aug. 2014. <http://www.engadget.com/2014/05/13/xbox-one-price-interview/>.

Gillespie, Tarleton. “The Politics of 'Platforms'.” *New Media & Society* 12.3 (2010): 1-18.

Grayson, Nathan. “Gamers Messed With The Steam Sale, Then Valve Changed The Rules.” *TMI*. N.p., 24 June 2014. 1 Sept. 2014. <http://tmi.kotaku.com/the-community-broke-the-steam-sale-so-valve-changed-th-1595087682>.

Greenwald, Glenn. *No Place to Hide Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books , 2015.

Grimes, Brad. “Data Mining: The Xbox Files.” *PC Mag*. N.p., n.d. 5 May 2014. <http://www.pcmag.com/article2/0,2817,1118791,00.asp>.

Guins, Raiford. *Game After: a Cultural Study of Video Game Afterlife*. Cambridge, MA: The MIT Press, 2014.

Haggerty, Kevin D., and Richard V. Ericson. “The Surveillant Assemblage.” *British Journal of Sociology* 51.4 (2000): 605-622.

Haggerty, Kevin D., and Daniel Trottier. “Surveillance and/of Nature: Monitoring Beyond the Human.” *Society and Animals* 1 (2013): 1-18.

Harbour, Jonathan S. *XNA Game Studio 4.0 for Xbox 360 Developers*. Boston, MA: Cengage Learning, 2010.

Hargreaves, Shawn. “Xbox Performances.” *Computer Graphics Laboratory*. N.p., n.d. 25 Aug. 2014. <http://graphics.ethz.ch/teaching/gamelab10/course_material/lecture03/03_XNA_Performances.pdf>.

Harper, Richard, and Helen M. Mentis. “The Mocking Gaze: The Social Organization of Kinect Use.” *CSCW â€™13* 1 (2013): 167-180.

Henson, Michael, and Stephen Taylor. “Memory Encryption: A Survey of Existing Techniques.” *ACM Computing Surveys* 46.4 (2014): 53:1-53:26.

Hollister, Sean. “Microsoft exec caught in privacy snafu, says Kinect might tailor ads to you.” *Engadget*. N.p., 26 Aug. 2011. 25 Aug. 2014. <http://www.engadget.com/2010/11/15/microsoft-exec-caught-in-privacy-snafu-says-kinect-might-tailor/>.

Huang, Andrew. “Hypervisor Privilege Escalation Vulnerability Â« bunnie's blog.” *Bunnie's blog*. N.p., 27 Feb. 2007. 25 Aug. 2014. <http://www.bunniestudios.com/blog/?p=159>.

“IBM Introduces Chip Morphing Technology.” *IBM News room*. N.p., 30 July 2004. 25 Aug. 2014. <http://www-304.ibm.com/jct03001c/press/us/en/pressrelease/7246.wss>.

Israel, Shel. “Why Apple Bought PrimeSense.” *Forbes*. N.p., 25 Nov. 2013. 1 Sept. 2014. <http://www.forbes.com/sites/shelisrael/2013/11/25/why-would-apple-buy-primesense/>.

Jackson, Steven J.. “Rethinking Repair.” *Media Technologies: Essays on Communication, Materiality and Society*. Cambridge, MA: MIT Press, 2014. 1-18.

Jakobsson, Mikael. “The Achievement Machine: Understanding Xbox 360 Achievements in Gaming Practices.” *Game Studies: The International Journal of Computer Game Research* 11.1 (2011): 1.

Jenkins, Gregory T., and Robert W. Bing. “Microsoft’s™ Monopoly: Anti-Competitive Behavior, Predatory Tactics, And The Failure Of Governmental Will.” *Journal of Business & Economic Research* 5.1 (2007): 11-16.

Kain, Erik. “UK Spies Considered Using Kinect, Microsoft 'Concerned'.” *Forbes*. Forbes Magazine, 28 Feb. 2014. 1 Sept. 2014. <http://www.forbes.com/sites/erikkain/2014/02/28/uk-spies-considered-using-kinect-microsoft-concerned/2/>.

Kean, Sam. *The Disappearing Spoon: and Other True Tales of Madness, Love, and the History of the World from the Periodic Table of the Elements*. New York: Little, Brown and Co., 2010.

Kirriemuir, J. “The Console Market.” *Virtual Reality* 5.4 (2000): 236-244.

Kravets, David. “First Criminal Trial Over Game-Console Modding Begins Tuesday.” *Threat Level*. Wired, 10 Nov. 1927. 25 Aug. 2014. <http://www.wired.com/2010/11/xboxmodding-trial/>.

Kushner, David. “Machine Politics.” *The New Yorker*. N.p., 7 May 2012. 25 Aug. 2014. <http://www.newyorker.com/magazine/2012/05/07/machine-politics>.

Lees, Jennie. “The Hypervisor and its Implications.” *Joystiq*. N.p., 25 Nov. 2009. 25 Aug. 2014. <http://www.joystiq.com/2005/11/29/the-hypervisor-and-its-implications/>.

“Llamma's Xbox 360 3RLOD (three red light error) X-Clamp Fix.” *The Llamma's Adventures in Xbox 360*. N.p., n.d. 25 Aug. 2014. <http://www.llamma.com/xbox360/repair/ring_of_light_x-clamp_fix.htm>.

Lowood, Henry. “Videogames in Computer Space: The Complex History of Pong.” *IEEE Annals of the History of Computing* 9.3 (2009): 64-71.

MacCormick , John . “How Does the Kinect Work?.” *Dickinson College*. N.p., n.d. 1 Sept. 2014. <http://www.dickinson.edu/>.

Maiberg, Emanuel. “What Big Data Can't Teach us About Videogames.” *Kill Screen*. N.p., 4 Nov. 2013. 25 Aug. 2014. <http://killscreendaily.com/articles/big-dada/>.

Massimi, Michael, Khai N Truong, David Dearman, and Gillian R Hayes. “Understanding Recording Technologies in Everyday Life.” *IEEE Pervasive Computing* 9.3 (2010): 64-71.

McHugh, Molly. “Kinect’s camera could record data for advertisers.” *Digital Trends*. N.p., 12 Nov. 2010. 1 Sept. 2014. <http://www.digitaltrends.com/computing/kinects-camera-could-record-data-for-advertisers/#!bNPuyA>.

“Microsoft Signs First NUads Advertisers, Including Toyota, Unilever and Samsung Mobile USA, on Xbox LIVE.” *Microsoft News Center*. N.p., 14 June 2012. 1 Sept. 2014. <http://www.microsoft.com/en-us/news/press/2012/jun12/06-14xboxadspr.aspx>.

“Microsoft's Xbox One video-game console sales hit 2 million.” *The Economic Times*. N.p., 23 Dec. 2013. 1 Sept. 2014. <http://articles.economictimes.indiatimes.com/2013-12-23/news/45510431_1_jack-tretton-david-dennis-washington-based-microsoft>.

Montfort, Nick, and Ian Bogost. *Racing the Beam the Atari Video Computer System*. Cambridge, Mass.: MIT Press, 2009.

Murakami Wood, David . “Beyond the Panopticon?: .” *Space, Knowledge and Power: Foucault and Geography*. Hampshire: Ashgate, 2007. 245-263.

Nasr, Magy Seif, Alessandro Canossa, and Anders Drachen. *Game Analytics: Maximizing the Value of Player Data*. London: Springer, 2013.

Nowak, Peter. “Video games turn 50 - Technology & Science.” *CBC News*. N.p., 15 Oct. 2008. 1 Sept. 2014. <http://www.cbc.ca/news/technology/video-games-turn-50-1.703624>.

Nutaro, James. *Building Software for Simulation: Theory and Algorithms, with Applications in C++*. Hoboken, N.J.: Wiley, 2011.

O'Donnell, Casey. “Getting Played: Gamification and the Rise of Algorithmic Surveillance.” *Surveillance & Society* 12.3 (2014): 349-359.

Petersen, Soren Mork. “Loser Generated Content: From Participation to Exploitation.” *First Monday* 13.3 (2008): 1.

Phillips, David. “Computer, Spatiality, and the Construction of Identity.” *Lessons from the Identity Trail*. Oxford: Oxford University Press, 2009. 303-318.

Pitcher, Jenna. “Killer Instinct will receive balance updates without patching.” *Polygon*. N.p., 10 Sept. 2014. 1 Sept. 2014. <http://www.polygon.com/2013/10/9/4819186/killer-instinct-will-receive-balance-updates-without-patching>.

Plunkeet, Luke. “This Kinect Patent is Terrifying, Wants to Charge You For License Violation.” *Kotaku*. N.p., 6 Nov. 2012. 1 Sept. 2014. <http://kotaku.com/5958307/this-kinect-patent-is-terrifying-wants-to-charge-you-for-license-violation>.

Quinn, Clark, and Lisa Neal. “Serious Games for Serious Topics.” *eLearn Magazine* 1 Mar. 2008: n. pag. *eLearn Magazine*. 5 May 2014.

“Sega scraps the Dreamcast.” *BBC News*. BBC, 31 Jan. 2001. 25 Aug. 2014. <http://news.bbc.co.uk/2/hi/business/1145936.stm>.

Sheldon, Lee. “About.” *Gaming the Classroom*. N.p., n.d. 1 Sept. 2014. <http://gamingtheclassroom.wordpress.com/>.

Sherman, JP. “Innovation or Invasion?” *The Escapist*. N.p., 8 Aug. 2011. 1 Sept. 2014. <http://www.escapistmagazine.com/articles/view/video-games/columns/first-personmarketer/9064-Innovation-or-Invasion.2>.

Sinclair, Brendan. “Gaming risks a repeat of 1983 crash - Report.” *GamesIndustry.biz*. N.p., 3 Oct. 2013. 1 Sept. 2014. <http://www.gamesindustry.biz/articles/2013-10-03-gaming-risks-a-repeat-of-1983-crash-report>.

Sinclair, Brendan. “Devs can't “create magic” with a spreadsheet in front of them.” *GamesIndustry.biz*. N.p., 11 Nov. 2013. 25 Aug. 2014. <http://www.gamesindustry.biz/articles/2013-11-11-devs-cant-create-magic-with-a-spreadsheet-in-front-of-them>.

Steil, Michael. “17 Mistakes Microsoft Made in the Xbox Security System.” *Proceedings of the 2005 Chaos Communications Congress*. N.p., 27 Dec. 2005. 5 May 2014. <http://events.ccc.de/congress/2005/fahrplan/attachments/591-paper_xbox.pdf>.

Street, Zoya. *Dreamcast Worlds: a Design History*. Oakland: Rupazero, 2013.

Tassi, Paul. “Microsoft's Yusuf Mehdi Explains The Xbox One's Split With Kinect.” *Forbes*. N.p., 13 May 2014. 25 Aug. 2014. <http://www.forbes.com/sites/insertcoin/2014/05/13/microsofts-yusuf-mehdi-explains-the-xbox-ones-split-with-kinect-2/>.

Tassi, Paul. “Microsoft May Be Looking To Sell Xbox Entertainment Studios To Warner Bros..” *Forbes*. N.p., 17 Aug. 2014. 1 Sept. 2014. <http://www.forbes.com/sites/insertcoin/2014/08/17/microsoft-may-be-looking-to-sell-xbox-entertainment-studios-to-warner-bros/>.

“Terms of Use.” *Xbox.com*. N.p., 14 July 2014. 25 Aug. 2014. <http://www.xbox.com/en-CA/Legal/LiveTOU>.

Terranova, Tiziana. “Free Labor: Producing Culture for the Digital Economy.” *Social Text* 18.2 (2000): 33-58.

The Conversation. Dir. Francis Ford Coppola. Perf. Gene Hackman. Paramount Pictures, 2000.

DVD.

Thompson, Clive. “Halo 3: How Microsoft Labs Invented a New Science of Play.” *WIRED*. N.p., n.d. 1 Sept. 2014. <http://archive.wired.com/gaming/virtualworlds/magazine/15-09/ff_halo?currentPage=all>.

Thorsen, Tor. “Xbox 360 failure rate 23.7%, PS3 10%, Wii 2.7% - Study.” *GameSpot*. N.p., 2 Sept. 2009. 25 Aug. 2014. <http://www.gamespot.com/articles/xbox-360-failure-rate-237-ps3-10-wii-27-study/1100-6216691/>.

Trottier, Daniel. “Crowdsourcing CCTV surveillance on the Internet.” *Information, Communication & Society* 1 (2013): 1-18.

Whitson, Jennifer. “Gaming the Quantified Self.” *Surveillance & Society* 11.1 (2013): 163-176.

Wills, Garry. *Bomb Power: the Modern Presidency and the National Security State*. New York: Penguin Press, 2010.

Witheford, Nick, and Greig Peuter. *Games of Empire: Global Capitalism and Video Games*. Minneapolis: University of Minnesota Press, 2009.

“Xbox Brings “Future-Generation” Games to Life.” *Microsoft News Center*. N.p., 10 Mar. 2010. 25 Aug. 2014. <http://www.microsoft.com/en-us/news/features/2000/03-10xbox.aspx>.

“Xbox LIVE Policies on Console Suspensions.” *Xbox.com*. N.p., n.d. 25 Aug. 2014. <http://www.xbox.com/en-CA/consoleban>.

Xynos, Konstantinos, Simon Harries, Iain Sutherland, Gareth Davies, and Andrew Blyth. “ Xbox 360: A digital forensic investigation of the hard disk drive.” *Digital Investigation* 6.3-4 (2010): 104-111.

Zimmerman, Eric. “Jerked Around by the Magic Circle - Clearing the Air Ten Years Later.” *Gamasutra*. N.p., 7 Feb. 2012. 25 Aug. 2014. <http://www.gamasutra.com/view/feature/6696/jerked_around_by_the_magic_circle_.php>.

Endnotes

[i] Parts of this thesis also appear in that volume of *Surveillance and Society*, in an article entitled "Enclosures at Play: Surveillance in the Code and Culture of Videogame" (Cybulski, 2014).

[ii] For example, Alessandro Canossa's *Reporting From the Snooping Trenches: Changes in Attitudes and Perceptions Towards Behavior Tracking in Digital Games* (2014) (cited in this thesis) which documents Canossa's observations of how game developers track player behavior in videogames, using his experience working with game developers.

[iii] Brighenti's analysis of visibility and representation on pages 175-176 is a helpful tool for analyzing surveillant gazes and would be useful in providing nuance to certain discussions of surveillance rooted in public/private visibility.

[iv] Because the design of each reporting structure is likely up to a game's developer or publisher how this memory closure is implemented. Subsequently, many techniques could be used to store this information, for example a value database could be substituted for a number of different memory enclosures to store this information, but serves as a good general example of how the data might be stored and retrieved for later use.

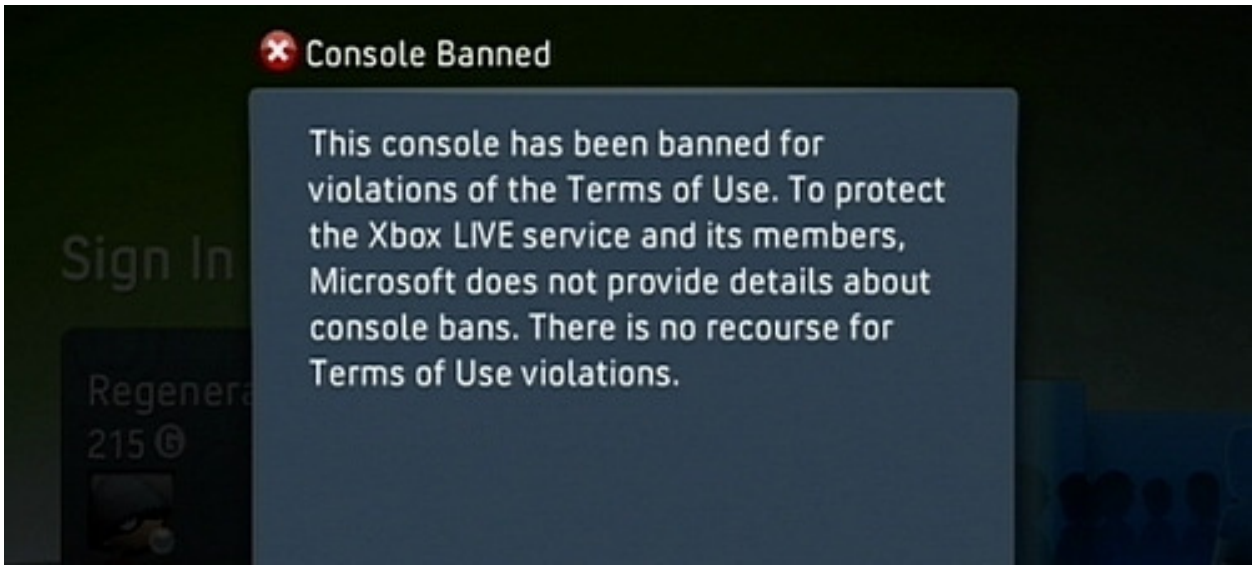
[v] For those unfamiliar with this kind of computer mischief: tampering with a save game file can be thought of in the same way a person might hack a bank account, creating imagined transactions that make it appear as if the user received substantial deposits. In the same way, gamesave tampering tricks game software into thinking that a user has accomplished certain objectives and in doing so, the software is then forced to attribute certain achievements to the user's account.

[vi] The trial, which began in 1998, dealt with Microsoft's uncompetitive control over the marketplace for operating systems and internet browsers. Despite losing the case, the findings of the anti-trust trial were still beneficial to Microsoft because it allowed the corporation to retain

much of its power despite its monopolies in the software industry. This is evident in Microsoft's ability to continue to expand horizontally across the software industry, specifically into games and the manufacture of videogame platforms like the Xbox.

[vii] It should be noted that Sony did not necessarily allow for Linux to be installed on the Playstation 2 for exclusively altruistic reasons. Among the factors contributing to the decision to support the operating system on its device were the high trade tariffs placed on videogame consoles in the European Union. By releasing kits of the Playstation that included Linux, Sony was able to argue that the Playstation was as much a computer as an entertainment device, successfully lobbying the EU for lower taxes and subsequently, a lower price for European videogame consumers.

[viii] http://www.ngohq.com/images/xboxban.jpg



[ix] https://www.ifixit.com/

[x] http://www.joystiq.com/2007/08/30/xbox-360s-get-new-warranty-seal-stickers/