Audio Beacon Technologies, Surveillance and Social Order

by

Iliyan Iliev

B.F.A. University of Colorado, Boulder, 2007

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
School of Interactive Arts and Technology
Faculty of Communication, Art and Technology

SIMON FRASER UNIVERSITY

Summer 2021

Declaration of Committee Page

Name: **Iliyan Iliev**

Degree: **Master of Arts**

Title: **Audio Beacon Technologies, Surveillance and Social Order**

Committee:

Chair:

Halil Erhan
Associate Professor
School of Interactive Arts and Technology

_____

Niranjan Rajah
Supervisor
Assistant Professor
School of Interactive Arts and Technology

_____

Sun-ha Hong
Committee Member
Assistant Professor
School of Communication

_____

Kate Hennessy
Examiner
Associate Professor
School of Interactive Arts and Technology

Abstract

This thesis explores audio beacon technology with the aim of elucidating the implications of this technology for the individual in contemporary society. Audio beacons are hidden inside digital devices. They emit and receive high frequency audio signals which are inaudible to the human ear, thereby generating and transmitting data without our knowledge. The motivation for this research is to raise awareness of the prevalence of audio beacon technologies and to explore their implications for contemporary society. The research takes an interdisciplinary approach involving – 1) a survey of audio beacon technology, 2) a contextualization in terms of contemporary theories of surveillance and control and 3) an interpretation in terms of 20th century dystopian literature. The hidden surveillance and privacy of this technology is examined mainly through the humanistic perspective of George Orwell's book *Nineteen Eighty-Four*. The general conclusion formed is that audio beacon technologies can serve as a surveillance method enhancing authoritarian and exploitative regimes. To mitigate the negative impacts of audio beacons, this research proposes two types of solutions – 1) individual actions that will have an immediate effect and 2) governmental legislation that can improve privacy in the longer term. Both of these solutions cannot happen without a raised public awareness, towards which this research hopes to make a contribution. Finally, this research introduces the notion of a 'digital paradox' in which the dystopian worlds of George Orwell and Aldous Huxley are brought together in order to characterize surveillance and control in contemporary society.

for my Father
who fought for democracy and
refused to surrender to authoritarian conformity
regardless of the price he paid

Acknowledgement

First and foremost, I want to thank Professor Niranjan Rajah for giving me a creative space, supporting my interest and for the nourishing wisdom and guidance that made this work possible. I'm also grateful to Professor Sun-ha Hong for the valuable input, the expertise and the insights into privacy and surveillance which were generously shared with me. Without you both this thesis would not have been possible.

This thesis also acknowledges all of you who toggle the privacy settings on your digital devices and choose not to share your data, choose not to use Google or Facebook and make tangible choices to increase privacy protection and thus preserving democracy.

Table of Contents

CHAPTER 1 – INTRODUCTION

"If you want a picture of the future,
imagine a boot stamping on a human face – forever"
(Orwell, *Nineteen Eighty-Four* 267)

1.1 – Audio Beacon Technologies

A few different names are used to represent the same audio beacon framework – ultrasound beacons, data over audio and uBeacons. Audio beacon technologies utilize a range of sounds[1] between 18 kHz and 20 kHz (Arp et al. 35). These high frequency sounds possess triple benefits – they are inaudible to humans, they are detected by other devices, and they have diminished interference with the human voice. According to Arp et al., "ultrasound … is a perfect match for designing an inaudible yet effective side channel between devices" (37). Audio beacons require a speaker and a microphone to transmit. All mobile devices contain these two components and they can transmit sound up to 44 kHz (Arp et al. 35, Vaghasiya et al. 413). Audio beacons do not require additional hardware nor do they depend on WiFi, Bluetooth, or network connectivity (Arp et al. 37, Vaghasiya et al. 416). The frequencies between 18 kHz and 20 kHz are divided into smaller units and a character or a symbol is assigned to each one of those units (Mavroudis et al.). Thus, audio beacons are able to transmit characters or symbols. The standard time that the ultrasound plays is one second. If a recognized beacon is detected, the data is transmitted to a server (Mavroudis et al. 97,98). This framework can be installed into any mobile app, which can play the inaudible sound unbeknownst to the user and simultaneously be detectable by other microphones.

1.2 – Audio Beacon Activation

A business owner can embed audio beacon technologies into their app without explicit disclosure. After the uBeacon is embedded, the app is made available for customer downloads. The first time the app is activated there is a request asking for

1 Sound travels in waveforms of varying frequencies. They are measured in units of Hertz (Hz) per cycle per second. Humans can hear sounds between 20 Hz and 20 kHz. Since hearing abilities decline with age, children experience a wider range of sounds than adults. Individuals 30 years of age and older have a hearing range usually capped around 18 kHz (Arp et al. 37). Some researchers report sounds to be inaudible to the human ear at 17 kHz (Constandache et al. 12).

microphone permission. Granting the app permission to the microphone in turn activates the audio beacon technology. The users are not aware when the microphone is being used, or the type of data transmitted to a server (Arp et al. 35), nor are they notified that the app will listen in the background (Mavroudis et al. 100).

1.3 – Data Transmission

The information transmitted includes device identity, model, IMEI, OS version, location, behavior of the user and other devices present (Arp et al. 36,38,40). Moreover, audio beacon technologies have access to all audible frequencies and are listening "even when the application has not been 'manually' started by the user" (Mavroudis et al. 100). There are only 2 ways of stopping the invasive framework – delete the app, or decline microphone permission[2].

1.4 – Contextualizing Biography

To understand the implications of audio beacon technologies for culture and society from a humanistic perspective, this thesis is going to examine the theoretical model created by George Orwell in his book *Nineteen Eighty-Four,* depicting the utilization of multiple surveillance technologies in the fictional world of Oceania. His dystopian vision of the surveillance state, written in 1949, reads like a prediction as the surveillance technologies have become the norm in today's world. However, Orwell's dystopian vision alone does not sufficiently portray the endless gamut of amusement choice found today. To create a broader perspective of audio beacon technologies, the last section of this thesis will address Aldous Huxley's book *Brave New World,* which illustrates a world engulfed by commercialization and entertainment. The juxtaposition of these two dystopian views offers a broader understanding of today's digital environment. I call this the *digital paradox*. The digital paradox is an amalgam of surveillance-based technologies and entertainment. Within this environment people freely explore the fastness of information the internet provides, but are being surveilled with every click.

Using Orwell's *Nineteen Eighty-Four* as a lens to examine social reality has been a concept grounded in my life experience growing up in a communist country. My

2 This situation resembles a scenario in chess called zugzwang. Zugzwang is a situation where the player is forced to choose between two bad moves. Deleting the app will obviously eliminate using it. The request for microphone permission is the last barrier for customers to avoid data transmission. Karyda et al. refer to it as "asymmetry of power" (203).

childhood experience in communist Bulgaria was happy and safe. However, from an early age, I was made aware of surveillance and inequality. My parents were not members of the Bulgarian Communist Party but were normal working-class people. They worked hard every day but after work their rebellious spirits emerged. Nightly at 8.00PM, my father prepared the radio by extending the antenna and used a stripped wire to connect it to the heating radiators. With the enhanced reception he could tune to Radio Free Europe. Although the reception was faint, appearing to come from another world, we gathered around the VEF 206 radio to hear the broadcast. The intermittent static contrasted with the warm and confident voice of the male commentator. Discussions centered around political events not covered by our local news: freedom of expression and surveillance. My parents ingrained in me the importance of secrecy as listening to this radio station was strictly prohibited and violators were imprisoned. This was my first exposure to the invisible gaze of the ruling party.

A few years later, Mikhail Gorbachev instituted Perestroika, and the ironclad dictate of censorship loosened its grip. Citizens were now able to admit they were listening to foreign radio stations. Western literature, previously banned, was now translated into Bulgarian, and George Orwell's book, *Nineteen-Eighty Four*, became available for the first time. The book became a cultural phenomenon. My group of friends and I inhaled it, drawing surveillance parallels within our own lives. As teenagers, we had nothing to hide from authorities, but we bonded in our attempts to employ rudimentary techniques of avoiding police patrols. However, we were unified in our apprehension to communicate our shared ideas with any known members of the communist party.

The book mirrored our adolescent, non-conformist desires. It also illuminated our perspective in regards to surveillance and oppression by making us aware of our limited freedoms in Bulgaria. *Nineteen Eighty-Four* helped us recognize the consequences that constant surveillance incurs and the potential paradigm resulting from the ubiquitous invasion of privacy.

Fast-forward a few years, I'm living in Denver, Colorado completing my Bachelor of Fine Arts degree. The exaltation of living in the USA was heady, yet tempered by two major events. The first being 9-11, the collapse of the World Trade Center in New York City and the subsequent laws enacted to eliminate privacy. Following that, Edward

Snowden conveyed in ordinary language how American lives had become a collection of data entered into an algorithm controlled by the government[3].

I regard privacy as a cornerstone of democracy, but in our digital age there has been an unmitigated assault upon it. The consequences of this are underestimated because the study of privacy diminishment is undervalued. I'm hopeful in the coming years that privacy laws will be further strengthened, forging a communal and undivided commitment to honor individuals' privacy. I would like to raise awareness of the use of audio beacon technologies along with their privacy implications thereby elevating recognition of the importance of persona data.

1.5 – Storyline of George Orwell's *Nineteen Eighty-Four*

The setting is the country of Oceania which is one of the three world powers in the narrative. The protagonist, Winston Smith, is a regular worker and one of the common ranking members of the ruling Party. The society of Oceania is managed and controlled by ubiquitous surveillance, enacted by telescreens and microphones. Additional surveillance methods employed are ground patrols, helicopters and encouragement of spying on family and friends. The dissidents are prosecuted by the Thought Police and after capture they either re-join society completely reformed or disappear entirely. The control of every aspect of society is further strengthened by propaganda, rewriting past events to correspond to current conditions and language use. Winston works for the Ministry of Truth and his job is to change past records to match current party policies. He yearns to join the subversive, rebellious movement known as the Brotherhood. In the course of the narrative Winston falls in love with Julia, who is another common ranking member of the Party. Both of them enjoy excursions to the country where they can be alone and unobserved. In order to avoid the inescapable surveillance of the Party, they rent a room above an antique shop. Simultaneously, Winston establishes a connection with O'Brien, a high-ranking member of the Party. Winston believes O'Brien is a member of the Brotherhood and O'Brien seems to confirm this by giving Winston a copy of the rebellious manifesto, a book written by the number one enemy of the Party, Emmanuel Goldstein.

---

3 Henry Giroux explores Prism and Tempura surveillance systems and the emergence of fusion centers ("Totalitarian Paranoia").

While in their private room, Winston and Julia make love and peruse items from the black market and read Goldstein's book. Both of them believe the room is free of surveillance because there is no visible telescreen. However, one day while in the room, Winston and Julia are caught by the Thought Police. It turns out that a telescreen was present in the room, but was hidden behind a picture on wall. Thus, Winston and Julia have not been watched by video, they have been audio surveilled. The audio aspect of telescreen surveillance proves to be effective and insidious in the narrative. Both of them are brought to the Ministry of Love, where Winston discovers that O'Brien is a high ranking member of the Thought Police who has been spying on him. Through a myriad of torture and brainwashing techniques, O'Brien slowly breaks Winston down. Eventually, Winston is taken to Room 101 where he encounters his worst fear – rats. Facing imminent death by rats clawing and gnawing on his face, Winston betrays Julia. He asks O'Brien to put her in his place. This act makes Winston's surrender to the Party complete and he is released back into society. He meets Julia, who confirms that she has betrayed him, too, and they both realize that everything between them is ashes. Alone in the local bar where he spends most of his time over a glass of Victory gin, Winston finally proclaims his love for the Party.

1.6 – The Focus of the Research

The object of the research is the societal impact of the emerging audio beacon technologies. This will be examined through two lenses. The first lens incorporates Orwell's dystopian novel, *Nineteen Eighty-Four,* and the second lens is surveillance theory as derived through the Foucauldian discourse on power. This approach is grounded in my own encounter with *Nineteen Eighty-Four* in the context of Communist Bulgaria and the fact that this novel enabled me to appraise and analyze the regime of surveillance that was the context of my youth.

The are two reasons why I'm using Orwell's book in the discourse on audio beacon technologies. First, the society portrayed in the book is subjected to constant and ever-present surveillance, achieved through several different means. Audio surveillance is one of the foremost methods and contributes to the demise of the central characters. The second reason concerns the collection of data. In the book, data is covertly accumulated over an extended period of time. The citizens have no indication that such activities are taking place. Audio beacon technologies collect audio data in a

similar way. By working in the background of mobile phones, the activity is indistinguishable to the owner. This research will also reflect on the capacity and limitations of Orwell's *Nineteen Eighty-Four* to offer insights on our contemporary society.

The second lens that will be used to contextualize the rise of audio beacons is the discourse on surveillance and privacy that derives from Foucault's observation on the 'disciplinary society' where power structures remain unseen, while people are constantly made visible by surveillance. For part of this discourse I will be using the writings of Shoshana Zuboff, Daniel Solove, Gilles Deleuze, Henry Giroux, Kevin Haggerty and Richard Ericson among others.

CHAPTER 2 – FIELD AND AREA

2.1 – The Social Impact of Technology

The research strives to raise awareness of audio beacon technologies through an interdisciplinary approach, which highlights the relationship between technology and the individual. David Edge sees technology and science as integrated into "human *achievements*"(4) that contribute to the critical evaluation and new interpretations of practices and institutions (15). He also studies aspects of authority and equality in human interactions and how science and technology can mitigate the power imbalance (Edge 16). Michel Foucault views technology as related to the power paradigm (qtd. in Maasen et al. 3,8) and Sergio Sismondo also explores the linkage between the dangers and benefits of technologies to social, political, economic and democratic affairs. Toscano elaborates that technologies might have social meaning assigned to them because societal values shepherd implementation of some technologies over others. His conclusion is technologies can be "read … similarly to how we read cultural works – art, literature, film, etc."(xii-xiii).

Michel Callon defines *extended translation* as a model that relates to processes forming a network, involving technology and individuals. This model not only produces statements, but also opens doors to conversations. Callon concludes that the strongest network is the one that incorporates various inner connections, because a potential validity inquiry is met with multiple translations that reinforce the findings (57).

To expose hidden elements, Joanna Radin uses the term "speculative present" (297), which exposes secret concepts behind the bifold vision of fact and fiction, inside and outside, content and form. Donna Haraway likewise blends the separation between fact and fiction – "the boundary between science fiction and social reality is an optical illusion" (8). Radin examines science and technology through fiction writing and forms a different way of understanding facts and new patterns of interpreting the power relationships in society. She applies the speculative present to the fiction writing of Michael Crichton to show covert aspects of the human-technology relationship in a "society seeking to regain its grip on reality" (Radin 315). The research strives to raise awareness of audio beacon technologies through an interdisciplinary approach, which highlights the relationship between technology and the individual.

2.2 – Methodology and Approach

Following Radin's example, this research will examine the emerging audio beacon technologies in order to understand their role in contemporary society. The hidden aspects of the human-technological relationship and the potential privacy implications of such technologies are explored through the perspective of George Orwell's dystopian science fiction novel, *Nineteen Eighty-Four*. While audio beacons can be embedded in many technologies including TVs, personal assistants, digital health tracking devices and IoT devices, they can also be implemented in a non-digital environments like malls, individual stores and buildings. This research is focused solely on the use of audio beacon technologies in mobile phones. It will examine audio beacon capabilities and the consequences of their use in mobile devices through a surveillance perspective. An interdisciplinary[4] approach is chosen, involving dystopian science fiction literature, on the basis that it can help put things in a humanistic perspective, while assisting us in comprehending the hidden aspects of the human-technological relationship and the potential privacy implications of such technologies. In addition to science fiction literature of the early 20th century, this research will incorporate secondary sources from the field of contemporary surveillance studies, which offer further perspective to the research topic. The approach adopted will involve literature review, analysis and theorization and is based purely on information that is freely available in the public domain from the sources listed herein – novels, monographs, peer-reviewed journal articles, conference proceedings, documentary films, websites, newspaper websites, statistical websites, magazine websites, corporate websites, policy documents and YouTube lectures series and videos.

2.3 – Surveillance Perspective and Choice of Literature

The various capabilities of audio beacon technologies will be observed first. Next, the research will examine the different ways the government of Oceania is surveilling its citizens in Orwell's *Nineteen Eighty-Four* and will focus on the audio technologies incorporated. The interpretation of these two elements through inductive reasoning will

4 Karyda et al. finds multidisciplinary approach necessary in research involving privacy protection, because it gives scholars "informed choices when exploring, designing or evaluating privacy protection schemes" (205).

help to synthesize an analysis about the manner in which audio beacon technologies can be used as surveillance technologies.

George Orwell's *Nineteen Eighty-Four* has been translated into over sixty languages (Slater xiv) and his writings in general (*Nineteen Eighty-Four* in particular) have had massive cultural impact. They have been used in history (Gitlin) and education (Bolin), sexual studies and gender identity (Rose), discussions regarding contemporary politics (Williams), analyses of Nazi and Soviet dictatorships (Dickstein), sociology (Rodden), pacifism (Rosenwald), race (Stewart), conformity (Sleeper), celebrity culture (Imber), the voice of the underprivileged (Hunter) and in film (Gottlieb). According to Slater, Orwell's work is not only nuanced but encourages multi-theme discussions (16). This thesis will incorporate Orwell's *Nineteen Eighty-Four* through a surveillance perspective. I'm also going to use additional literary material which contextualizes *Nineteen Eighty-Four* in regards to surveillance and privacy. Orwell wrote the book in 1949 in London, in the aftermath of the Second World War. It is logical to argue that the world vision in the book resembles the totalitarian governments erected in Nazi Germany and Stalinist Russia. Both of those regimes were characterized by the "smother[ing] of the individual" (Slater 16). According to Slater, Orwell situated the book in England, because he did not consider England exempt from such political destiny (xii). To Orwell, the fight against totalitarianism ought to be perpetual because the tendencies can exist in any political and social environment and can corrupt democracy from the core (Slater xiii). *Nineteen Eighty-Four* is the most influential and popular of Orwell's works (Slater xiv). In the year it was released, it sold half a million copies (Slater 15).

Orwell's vision in *Nineteen Eighty-Four* will be used as a model of an opulent surveillance state which incorporates different methods of control. My personal experience with *Nineteen Eighty-Four* will serve as a base to reflect on the literature again and to bring new insights. My findings include the distinction of five different methods of surveillance – ground patrols, helicopters, encouraging self-spying among citizens, video surveillance and microphones. These methods are aided by another three factors of manipulation – language use, propaganda and altering the past. However, this thesis is not going to engage in literary criticism, but rather incorporate Orwell's *Nineteen Eighty-Four* as a lens in a multidisciplinary approach. Another finding is that the perception of the proles neighborhood being free of surveillance is inaccurate. This is Winston's view in the book and his assumption is wrong. The proles' neighborhood is

falsely advertised by the Party as a surveillance free zone in an attempt to capture dissidents.

Three companies developing audio beacon technologies (Lisnr, Shopkick and Silverpush) will be explored. All three companies utilize Google cookies for their functionality. Since Google is an American corporation and is under the United States jurisdiction, a brief history of privacy in the United States will help us to understand the historical aspect. This section of the thesis will be aided by Sarah Igo's book *The Known Citizen*. To understand Google's marketing practices and business model, I'm going to turn to Shoshana Zuboff and her book *The Age of Surveillance Capitalism.* Zuboff's book will be used to raise a more contemporary theoretical understanding and placing audio beacons in the contemporary social environment.

Further, the surveillance technologies and the insight given by the fictional literature will be juxtaposed with theoretical observations and the questions of power arising from Michel Foucault in *Discipline and Punish*. Foucault's societal observations will help us cross cultural boundaries and explore processes of control that are similar in different societies. Foucault's observations on power in his book *Power/Knowledge* and the work of various scholars whose analysis is derived from them, will assist us to understand the methods and motivation behind the power imbalance created by covert surveillance technologies such as audio beacons.

To create a complete picture of the social paradigm today, this research will be aided by another work of dystopian futurist literature, Aldous Huxley's *Brave New World*. Huxley's book will support the understanding of contemporary society and it's incorporation of entertainment and commercialism.

Seen through these lenses, an ethical, social and privacy perspective on audio beacons will emerge.

2.4 – Outline of Narrative Structure

The thesis will follow the four act narrative structure with the elements of rising and falling action. The Setup, the establishment of the situation, will be covered in Chapters 3 and 4. Chapter 3 will focus on in-depth analysis of the five surveillance methods described by George Orwell in *Nineteen Eighty-Four*. They will be juxtaposed with contemporary surveillance counterparts in use today. Chapter 4 will focus on a comprehensive explanation of audio beacon technologies, their capabilities and related

consequences. Chapters 5, 6, 7 and 8 will be dedicated to the development of the argument. Chapter 5 will examine audio beacons as surveillance technologies and the environment of web surveillance today. To diminish the association between Big Brother and surveillance concepts and to show that privacy and surveillance are not associated solely with digital technologies, Chapter 6 will offer a brief historical overview of privacy in the USA and in Orwell's *Nineteen Eighty-Four*. This chapter also will explore audio beacon technologies in relation to Helen Nissenbaum's theory of privacy as contextual integrity. Chapter 7 will demonstrate that privacy and surveillance practices are present across multiple societies. This chapter will utilize Michel Foucault's book *Discipline and Punish* and explore three aspects of the disciplinary power structure – punishment, surveillance and the resulting rise of comprehensive documentation. I'm going to explore the societal order in *Nineteen Eighty-Four* and the role audio beacons play in the societies of control. Inserting audio beacon technologies in our contemporary paradigm, Chapter 8 will scrutinize surveillance practices and Surveillance Capitalism. This chapter will explore Zuboff's book *The Age of Surveillance Capitalism* integrating her idea of "The Big Other" ("Big Other" 81), while also covering the economy of audio beacons. The Culmination of the narrative will be found in Chapter 9. To create a holistic picture, this chapter will link Orwell's *Nineteen Eighty-Four* and Huxley's *Brave New World*. Within Chapter 9, the reader will discover a synopsis of Huxley's Brave New World and a description of Orwell's war society. This chapter will survey Neil Postman's book *Amusing Ourselves to Death: Public Discourse in the Age of Show Business.* However, the approach will differ from the description by Postman. Postman's perspective is that both books present opposing visions, while this thesis views both books as complimentary. This approach will give us a more complete understanding of contemporary society. To assess modern social order, an evaluation of the dichotomy between security and privacy, *entertainment surveillance* and the use of language will be taken up as well.

The Resolution, delving into motivation behind the use of audio beacons and proposed solutions, will follow in Chapter 10. This chapter will also explore the motivation of the ruling Party in Orwell's *Nineteen Eighty-Four.* Here the reader will find Foucault's exploration of how new information creates new knowledge and the power-knowledge system that necessitate each other. The end of the chapter will carry the Conclusion and the Findings. The Epilogue will consist of Chapter 11, where having used Orwell as a

lens in the examination of audio surveillance in contemporary society, I will offer some reflection of interpretative potential of dystopian science fiction. I propose that contemporary society can be described as the *digital paradox.* Present day digital societies employ mass surveillance with new forms of entertainment entwined in paradoxical connection. In Huxley's *Brave New World* and Orwell's *Nineteen Eighty-Four,* mass surveillance and entertainment technology do not exist in the same society. In order to understand contemporary social order, I will analyze a combination of both visions. Here Orwell's symbol of surveillance and oppression will be connected with Huxley's method of control. The digital paradox will be connected to Foucault's discipline societies.

CHAPTER 3 – SURVEILLANCE AND SOCIAL ORDER IN ORWELL'S *NINETEEN EIGHTY-FOUR*

3.1 – Introduction to Surveillance

Surveillance involves the act of looking at or listening to a certain person, event or situation. This act of observation is not innocuous, instead the observer strives to collect detailed data, to identify correlations and to assemble the data into meaningful units. Early on, parents monitor their children in their cribs with audio devices. Today audio-video tools are the norm. As the child grows, this mode of observation will incorporate continual behavior corrections by the parents. The child is molded to learn and perform the proper behavior that society expects, as well as obeying cultural norms. This mode of observation analysis and parental critique intensifies with age. Teenagers can be subjected to parental controls on their digital devices and parents may choose a more severe form of surveillance by installing tracking apps on their children's phones and in the cars they drive. Paradoxically, this stage of quiet surveillance also winds its tentacles around the parents at their workplace. The rabbit hole continues endlessly as the people that monitor the workers are monitored themselves by someone else. Thus, surveillance asserts a power structure pregnant with hierarchy, control and social order. Surveillance is not a new byproduct of the digital society, it has been around for centuries (Crawford and Joier, "Anatomy" VII).

3.2 – Modes of Surveillance in Orwell's *Nineteen Eighty-Four*

The dystopian world created by George Orwell in his book *Nineteen Eighty-Four* is so wildly renowned that it might be deemed a cliché to compare the fictional state of Oceania with contemporary surveillance practices. However, Lonneke van der Velden sees a shift away from the cliché perception with the emergence of "data bodies" (183) and the prediction model of behavior. Wood and Caluya also reference the rooting of surveillance studies today in the "post-Foucauldian paradigm" (qtd. in Velden 183). To realize how the government of Oceania eliminates meaningful revolt, this section of the research will re-examine the web of surveillance practices used to control the population. Further, juxtaposition of those methods along with contemporary counterparts will be employed.

The ruling party of Oceania uses five different yet synchronized surveillance methods to exert their authority – ground patrols, helicopters, encouraging self-spying among citizens, video surveillance and microphones. These methods go further with additional aspects of manipulation – language use, propaganda and altering the past. These three additional aspects of control will be examined in Chapter 9.

3.2.1 – Ground Patrols

The ground patrols first appeared in the book when Parsons bragged about his daughter following a stranger and that she "handed him over to the patrols" (Orwell, *Nineteen Eighty-Four* 57). Patrols are present in the proles sections of the city, "railway stations" (Orwell, *Nineteen Eighty-Four* 117) and on the streets - "patrol had just come around the corner" (Orwell, *Nineteen Eighty-Four* 129). These patrols are on Winston's mind constantly as he tries to circumvent them. Curiously, he was never intercepted or questioned by them, which leaves us with the notion that patrols are not very effective at preventing suspicious activities. To address this concern, patrols on the ground are assisted by a complimentary force – helicopters.

Ground patrols in many ways resemble modern day law enforcement. This mode of surveillance is not considered bad, but necessary to prevent crime. In addition, law enforcement is enforcing the social order by observing. In the case of Oceania, they are also preventing mobility from town to town and within the city (Orwell, *Nineteen Eighty-Four* 117,179).

3.2.2 – Helicopter Policing

This mode of surveillance is minimally explored in the novel. Helicopters intrude on the citizens directly by observing them through their windows. This technique of observation appears to be ineffective, yet somewhat overvalued. The blatant tactic makes sense if it is viewed as a tool of intimidation. Contrarily, helicopters can gather valuable data by flying at a higher altitude so as not be seen or heard. Today, this mode of surveillance is present and thriving. According to Burgin, in 2011, Rodney Brossart was the first known person to be arrested in the USA because of drone surveillance (1135). Gillum et al. and former FBI agent David Gomez confirm that drones are used to help ground forces. In addition to recording high definition video, another technology called Stingray is also used. According to Knappenberger, *The Stingray* imitates a cell

phone tower so mobile phones in the vicinity connect automatically (00:08:45-00:09:40). The technology does not relay phone calls, but rather transmits the phone's information to their server, regardless if the phone is in use. Rachel Finn and David Wright investigate the use of unmanned aircraft systems (drones) in cities. The researchers observe that these drones are going undetected by the populace because of their noiseless operation and invisibility (qtd. in Friedewald et al. 10,11). The FBI does not discriminate tracking of the target phones, but gathers information from thousands of people in the area, even those unrelated to criminal actions.

3.2.3 – Encouraging Self-Spying Among Citizens

All citizens in Oceania are encouraged to spy on their neighbors and co-workers, including their immediate families. In this society, only one group of people are shown to successfully practice this activity – the children. "It was almost normal for people over thirty to be frightened of their own children" (Orwell, *Nineteen Eighty-Four* 24). Children are supplied with helpful instruments – "Ear trumpets for listening through keyholes" (Orwell, *Nineteen Eighty-Four* 63), making spying easier for them. In doing so, "The family had become in effect an extension of the Thought Police" (Orwell, *Nineteen Eighty-Four* 133). This unnerving mode of observation creates an atmosphere of constant alertness and suspicion among family and friends.

Spying and reporting on friends and family has been a part of recent American history as Sarah Igo finds in her book *The Known Citizen*. The hearings of the House Un-American Activities Committee in the mid 20th century blatantly encouraged the exposure and betrayal of colleagues and friends that might be involved in Communism (Igo 101). This practice of snooping proceeded into the suburbs where agents would gad around, speaking to anybody that was willing to rat out their neighbors (Igo 114).

Shoshana Zuboff, in her book *The Age of Surveillance Capitalism,* reports that in 2016 Google employed a company-wide spying program that encouraged co-workers to report confidentiality violations (64). Following this, the Obama administration founded the Insider Threat Program, which solicited government workers to spy on each other and report colleagues for refusing to participate (qtd. in Giroux "Totalitarian Paranoia" 121).

The magnitude of this surveillance technique can be observed by studying the largest social media platform today – Facebook (Statista). Statista reports Facebook

active users for the fourth quarter of 2020 to be over 2.7 billion. Thus, policies implemented by the social platform impact an enormous amount of individuals. Grimmelmann concludes that privacy violations on social networking sites are mainly caused by employer and administrator “snooping” (qtd. in Rubinstein and Good 1347,1348). When asked about the use of legal or preferred names on the site, the co-founder and CEO of Facebook, Mark Zuckerberg, says: “You have one identity … Having two identities for yourself is an example of lack of integrity” (West 34). His views are explicitly supported by the company’s “automated reporting feature enabling users that violate the policy to be flagged by other users” (West 34). According to West, this Facebook method of encouraging family and friends to report on each other, “has resulted in broad discrimination against certain communities, including members of the transgender and Native American communities” (34,35). Orwell warns us of this mentality and its consequences in 1949 – “[spying on your own family] was a device by means of which everyone could be surrounded night and day by informers who knew him intimately” (*Nineteen Eighty-Four* 133).

3.2.4 – Video Surveillance

The most substantial and certain spying technique in Oceania is video surveillance. Throughout Orwell’s book we discover that video screens are placed ubiquitously – in public spaces, in work environments, in lobbies of residential buildings, in hallways, in elevators and inside people’s homes. This relentless surveillance scrutinizes every aspect of individual’s lives. The telescreens are capable of transmitting and receiving both video and audio and the option of turning them off does not exist.

The pervasiveness of video surveillance practices in public environments is a topic covered by many researchers - surveillance in public squares (Valenzise et al.), surveillance in railway stations (Zajdel et al.), surveillance in public transport vehicles (Pham et al., Rouas et al., Vu et al.), surveillance in elevators (Radhakrishnan et al., Teck Wee Chua et al.) and surveillance in offices (Harma et al., Atrey et al.). The digitization of the modern world has made surveillance omnipresent and normal. A surveillance device lacks bias, it monitors and collects data of everything in its reach. A camera, unobtrusive in its demeanor, surveils individuals regardless of weather conditions, social status, profession or education. Citizens of Oceania are monitored relentlessly due to suspected subversive activities. If we apply the same principle today,

continually surveilling non-criminals, the law of innocent until proven guilty becomes a sham.

3.2.5 – Audio Surveillance

In addition to the spying technologies mentioned above, the Thought Police also implement microphones to spy on all individuals of Oceania. Aforementioned video screens are all equipped with microphones – “He thought of the telescreens with its never-sleeping ear” (Orwell, *Nineteen Eighty-Four* 166), but those devices leave a large portion of the environment unobserved – the countryside. The rural areas are monitored by microphones – “There were no telescreens, of course, but there was always the danger of concealed microphones” (Orwell, *Nineteen Eighty-Four* 117). This mode of surveillance is the only one that depends on inconspicuous technologies. Elizabeth Stoycheff shows that surveillance changes human behavior (12). Therefore, the hidden mode of observation would be the most authentic because it captures the uninhibited individual. The room at Mr. Charrington’s shop is a sanctuary where Winston and Julia can strip away their facades of brainwashed parasites and express sincere thoughts and emotions. In this room they consume black market items and Winston reads Emmanuel Goldstein’s book. In essence, Winston and Julia could be themselves only when they had privacy. Mr. Charrington, a superior member of the Thought Police, understood best the significance and importance of a sanctum – “Privacy, he said, was a very valuable thing. Everyone wanted a place where they could be alone occasionally” (Orwell, *Nineteen Eighty-Four* 137). Winston and Julia assumed they were safe here, because there was no telescreen. As it turns out, the telescreen “was [concealed] behind the picture,” said the voice” (Orwell, *Nineteen Eighty-Four* 221). Therefore, the telescreen, while hidden, was unable to scan the room, but it was listening and surveilling the occupants. Winston and Julia were not watched, but listened to. This method of concealed surveillance is used to make Winston reveal his most intimate fear – rats. Using this, the Party forced him to irreversibly betray what he cared about the most, his love for Julia.

The authoritarian regime in Oceania is possible with widespread implementation of surveillance technologies. Amongst these, the covert audio surveillance technologies are the most effective.

CHAPTER 4 – AUDIO BEACON TECHNOLOGIES AND THEIR CAPABILITIES

4.1 – Location Tracking

Several audio systems can locate mobile devices within centimeters with a fixed beacon in the environment (Aguilera et al., Lopes et al., Constandache et al.). Other unbinding systems determine locations from ultrasounds emitted by mobile devices (Filonenko et al. and Arp et al.); BeepBeep system, developed by Peng et al., is able to achieve location accuracy of 1-2 cm; Constandache et al. developed their Daredevil system capable of simultaneously detecting 40 phones every 30 seconds within 35 feet; and Hon et al. solves the self-localization problem of random mobile phones in outdoor environments with heavy noise and low reverberation (concerts) using audio fingerprinting methods. Further, using audio to localize devices does not depend on the device position or orientation (Hon et al. 1623).

Arp et al. examine three companies – Lisnr, Shopkick and Silverpush. The first two companies use audio beacons in mobile apps for location tracking, while Silverpush uses inaudible sound for media monitoring and cross-device tracking. Mavroudis et al. adds a few more businesses to the list of audio beacon companies – Google Cast, CopSonic, Signal360, Audible Magic (95,96). Arp et al. looked at the "communication protocols and signal processing" (35) of these companies and found apps listening for ultrasonic beacons in the background without user awareness. Location tracking is transmitted without the use of Global Positioning System (GPS) (Arp et al. 36) and includes longitude and latitude (Mavroudis et al. 96). Silverpush claims tracking 18 million devices in 2015 (Zeppelzauer 1250) and Aguilera et al. had said that their centimeter precise localization system is to be used in museums, malls and airports.

When we work with such precise location accuracy (less than 10 centimeters), other dimensions can be established. Implementing algorithms in combination with educated guesses, one can deduce users' actions and activities. Location tracking can reveal where an individual sleeps and stays for long periods of time and deductions can be formed about who they spend time with (Arp et al. 36). Ashbrook and Starner have developed an algorithm that successfully predicts future movement of the users based on location tracking. The researchers were able to deduce significant locations for each user based on the previous two locations visited. Ashbrook and Starner were able to

predict the behavior of the users and their next destination. Location data helped, the researchers were also able to predict if certain people were going to meet. The results of the research show that the algorithm worked with both single and multi-user prediction and "showed relative frequencies significantly greater than chance" (Ashbrook and Starner 285). Heerden et al. reports that Facebook had identical research with their patent called "Offline Trajectories" (2). Based on users' location and Facebook data, the company was able to predict the future movement of individuals. Thus, location data (regardless of how it is generated) largely determines human behavior and the collection of location data allows companies to predict what a user is going to do next, before the user knows themselves (Ashbrook and Starner).

4.2 – Cross-device Identification

Devices emitting audio beacons continuously detect other devices in the vicinity. It's simple to deduce that those devices belong to the same individual. Thus, the behavior of users can be monitored across multiple devices. Further, the information establishes a connection between work and personal devices, which has privacy and security implications as well. (Arp et al., Mavroudis et al.). The Chief Marketing Officer and co-founder of Silverpush, Mudit Seth, confirms it by saying "We are able to match 70 to 80 percent of desktop users to their mobile phones" (qtd. in Taslima 3). Other companies like Google, Tapad and Drawbridge explore audio cross-device tracking technologies as well (Taslima 1,3).

4.3 – De-Anonymization

The implementation of audio beacons allows the de-anonymization for Bitcoin and Tor users. The ultrasonic signal can establish a connection between the real location of the device, the actual user and the Bitcoin address. This reveals the individual's identity (Arp et al. 37). Mavroudis et al. finds the same for Tor and VPN users (96). The research also uncovers the vulnerability of ultrasonic technologies to de-anonymization attacks, not only by the companies that manufacture them, but third parties as well (Mavroudis et al. 102). De-anonymization is made possible by the beacon's continuous listening mode, which captures human voices. According to Pathak, the unique characteristic of every human is revealed by the sum of that person's voice and the way they speak (qtd. in Crocco et al. 37).

4.4 – Media Tracking

Silverpush is aiming to track users' TV viewing habits. The ultrasound beacon can transmit watched content data, time, location, broadcast channel and the duration of the viewing. Thus, the viewing behavior of the individual is connected to their mobile devices. Highly sensitive viewing habits of individuals can be revealed across multiple devices and locations (Arp et al. 36). The research by Ka et al. is improving media tracking by beaming additional information to the user's mobile phone based on the program being watched.

4.5 – Trigger Actions

Vaghasiya et al. propose an inaudible beacon triggering system. Sounds emitted by any speaker lasting only 0.0005 to 0.002 seconds can trigger predetermined actions on a smart phone without any interaction with the user. The sound can be played on a loop continuously, or when the desired action is required. One transmission can activate multiple devices (Vaghasiya et al. 414,418). The actions can display an advertisement, push notifications or load a predetermined web page. More invasive actions include – changing sound profiles, enabling location tracking, and WiFi and Bluetooth toggling. The researchers claim that their system can be employed in speakers, shopping malls, TV and radio commercials, children's toys, classrooms, concerts and public spaces. It can also be embedded into any mobile phone application and even functions in airplane mode. The proposed system also keeps a history log of all the triggering activities and transmits them to the local server (Vaghasiya et al. 415). As Vaghasiya et al. state, "This kind of implementation by marketers can not only provide rich and immersive experience but also help them with user tracking and analytics" (417).

4.6 – Utilization

The implementation of audio beacon technologies is marketed as an advertising tool, but as established prior, has far-reaching privacy and surveillance concerns (Arp et al. 35, Mavroudis et al. 107). The utilization of those technologies is growing. Between April and December 2015 the apps that implement audio beacons have jumped from 6 to 39, and to 234 apps by January of 2017 (Arp et al. 35,43). These numbers might not seem significant, but remember that one single app is downloaded millions of times. Samara Lynn reports 50 million interactions using Lisnr in 2016, and the CEO of the

company, Rodney Williams, states that their audio beacon technology works with Internet of Things (Lynn). Even though Arp et al. did not discover any TV content using audio beacons in 2015, the trend is alarming (37). Since users are unaware that ultrasonic beacons exist on their devices, they avoid detection. This observation is supported by the fact that apps are not indicating their implementation of ultrasonic beacons and the signals themselves are not showing any signs of listening in the background (Arp et al. 41,42).

CHAPTER 5 – AUDIO BEACON AS SURVEILLANCE TECHNOLOGIES AND THE WEB OF SURVEILLANCE

5.1 – Brief Overview of Audio Surveillance

Josh Lauer dates the groundwork for audio surveillance to be placed in the late 19th century through the invention of the phonograph and the telephone. Both these technologies offered new ways of knowing an individual (Lauer 570). The phonograph was invented in 1878 by Thomas Edison and sound recording commenced. Promoting the new technology, Edison announced that the phonograph can be used to record people with or without their consent (qtd. in Lauer 573). He further elaborated that the recordings could be copied and preserved for posterity without the approval of the "original source" (qtd. in Lauer 573). The potential surveillance capabilities of the phonograph were recognized immediately, describing it as a tool for voice identification, proof of one's thoughts, feelings and actions (Lauer 575).

The telephone was patented in 1876 by Alexander Bell and was perceived as a tool of "spacial invasion" (Lauer 576). Eavesdropping was an inherent feature of the early telephone, because operators were involved in connecting both parties. Furthermore, the operators had to validate that the connection was successful and verify that the parties ended the conversation so the switchboard could be disconnected (Lauer 576). The eavesdropping intensified when party lines were introduced and up to ten families were part of the same line (Lauer 576).

The first part of the 20th century presented another device that contributed to eavesdropping and gradually progressed as a detective device, the dictograph (Pavlounis 36). The dictograph was marketed as a business tool that allowed managers to relay orders to numerous subordinates simultaneously and without the need of direct contact (Pavlounis 38). Dimitrios Pavlounis sees this aspect of the dictograph as contributing to the power imbalance between management and the workers (37). The dictograph was able to hear and transmit even the faintest of human sounds. A new version of the device was introduced in 1910 called the detective dictograph (Pavlounis 40). This portable version was designed specifically for surveillance, allowing unidirectional communication only. It prevented unintentional audio disclosure of the eavesdroppers (Pavlounis 40). Technological advances of audio transmission and magnetic wire allowed the incorporation of wire recorders and electronic surveillance in

the mid 20th century (Pavlounis 133). However, during the Second World War, German technology advanced surveillance monumentally. The Magnetophon, incorporating magnetic tape recording, improved sound quality and fidelity (Pavlounis 134). After the war, the technology was exported to the USA and by the mid-1950s tape recorders were in wide use by police (Pavlounis 137). By the early 1960s the consumer tape recorder was in mass use in the USA (Pavlounis 188). This device implemented micro-transmitter and a directional microphone which made audio recording very easy. Tape recorders also used transistors, shrunking them to a miniature size, enabling them to be hidden in watches, cigarette boxes and most famously, in a martini olive (Pavlounis 191).

Julie Petersen also finds the invention of the transistor to be the ultimate technological development, that expanded contemporary technology (20). The transistor made possible the development of portable radio technologies, which in turn made satellite communication possible. She recognizes the launch of the SCORE satellite in 1958 as an example of stretching audio communication over vast distances without the need of wires or connecting stations (Petersen 22).

This brief historical overview demonstrates that audio surveillance is not a new environment enabled by digital technologies. Rather, contemporary surveillance technologies are a continuation and expansion of previous technologies. Although one distinct difference is evident – the development of audio beacons bypasses the targeted surveillance practices of previous decades and enables mass scale surveillance of users.

5.2 – The Importance of Audio Surveillance

Audio beacon technologies listen, record and transmit sounds in their range. Their capabilities show that contemporary audio technologies are advancing the surveillance paradigm even further than Orwell imagined. The question arises – is audio spying necessary when video cameras are present? The following research gives answers to that question. The research on audio histograms by Reddy et al. states - “human beings express their emotions like happiness, sadness, anger, panic, shock, and surprising events in terms of different forms of speech … Hence, most of the acoustic events in human presence can be detected from the speech signals” (1978). Irwin Altman expands that individuals become easier to distinguish due to their oral

expression and its audio qualities of pitch, tone and intensity, thus compromising privacy (qtd. in Rubinstein and Good 1369, 1370).

Further, the research by Crocco et al. finds real world video surveillance not to be sufficient and reliable enough if it's used alone without the support of additional sensory trackers. Video surveillance has been strongly enhanced with audio while audio-only devices continue to be implemented as a separate surveillance strategy. While video records our external state, audio discloses an intimacy of our internal state. Health conditions may be revealed as well as mental state and live dreams. Consequently, audio data becomes more valuable than ocular data. Crocco et al. states five other practical reasons – 1) audio requires less bandwidth and storage, 2) omni-directional microphones capture audio 360 degrees, 3) audio bounces off of surfaces allowing capture despite obstacles, 4) "illumination and temperature" (52:2) are not concerns and 5) incidents involving screams are undetectable when out of view.

5.3 – Web of Surveillance

By subjecting individuals to five forms of surveillance, George Orwell creates the ultimate surveillance domain. Citizens of Oceania are inundated by tracking devices from every direction. Contemporary surveillance technologies are on steroids up against Orwell's vision from seventy years ago. Although research has shown that big data companies are able to manipulate elections (Tufekci, Zittrain), designating them as the sinister Big Brother requires a giant leap. Therefore, individuals rarely see the value of their own data. Luke Stark defines this blind spot of perception as "data myopia" (21). Data myopia prevails because individuals do not comprehend how their data grows or witness any negative consequences because companies are not disclosing how they are using the data. Effectively, people fail to form a crucial bond with their own data (Stark 21) allowing a state of data capitalism to develop (West 20). Sarah West views this data aggregation of gestures and utterances to be an imbalanced territory with an "asymmetric redistribution of power" (20). These conditions enable the growth and the advancement of corporations, which expand capital and motivate development of additional invasive technologies. Consumer data is valued by the existence of data brokers who buy and resell the commodity (West 31). Companies' methods of attaining personal data are not available for examination, personal consent or legal action, because the practice is hidden from public view (Zuboff, "Big Other" 78). Surveillance

and tracking technologies create environments where the individual is unfailingly visible, or, as Haggerty and Ericson coin, the state of “disappearance of disappearance” (619). The commerce of personal data is facilitated by the free market economy which then enables data aggregation in the same organization (private, public of governmental). This data gives the organization a comprehensive picture of the user. Implementing this knowledge, the business can manipulate individuals to further their own agenda. Big Brother has just become a small step within the organization’s culture. Brey warns us that surveillance technologies could empower a society to become the Oceania Orwell describes in *Nineteen Eighty-Four* (qtd. in Karyda et al.195). Heerden et al. identify such a system already in effect in China. The country instituted a social credit system which uses mass surveillance to monitor the financial and social standing of its citizens. The data is classified into a social score, which is used to control the population through rewards or discipline (Heerden et al. 7). The researchers recognize this system of control has an “Orwellian feel” (Heerden et al. 7). Grounded in the above-mentioned importance of audio surveillance, I would argue that audio beacons, as an acoustic-based surveillance technology, have privacy and sociopolitical implications. Further, the implementation of audio beacon technologies allows mass scale surveillance by covert listening of mobile phone users.

CHAPTER 6 – BRIEF ACCOUNT OF PRIVACY HISTORY IN THE USA

The three companies developing audio beacon technologies explored in this thesis are Lisnr, Silverpush and Shopkick. All three of them are using Google cookies for their functionality. Google's headquarters are located in Mountain View, CA thus the corporation falls under the jurisdiction of the USA. Meaning, the United States' notions of privacy and legislation directly impacts the implementation of audio beacons. It can be argued that every country has its own privacy policies and American corporations have to abide by them. However, recent lawsuits show that Google does not yield to those regulations (Noyb, "Austrian," "Data Transfers") and that some countries are not enforcing those laws against Google (Noyb, "Luxemburg"). Further, recent trends of multiple lawsuits in the European Union against Google and Facebook show that these companies strive to by-pass legislations until they are challenged in court (Noyb "101 complaints," Noyb "Breaking," Zuboff "Big Other" 78). This situation leaves one simple and robust solution – the passing of privacy regulations in the United States. As such this thesis will focus on the privacy history in the United States only. This brief overview will help us place the implications of audio beacons in a historical perspective. Privacy in Oceania will also be covered and the chapter will conclude with the examination of audio beacon technologies through Helen Nissenbaum's theory of privacy as contextual integrity.

We will use as our foundation the widely recognized definition of privacy as penned by Alan Westin - "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (qtd. in Rubinstein and Good 1347). This definition is appropriate for the thesis, because data transmission of audio beacons is a constant. Their usage eliminates the user's control over the flow of data to unknown parties and eliminates the user's choice to control how, when or what is transmitted.

6.1 – Privacy in Oceania

The omnipotent surveillance practices in Oceania result in complete deprivation of individual privacy. Winston and Julia do not journey to the countryside to enjoy the scenery, they are motivated by the lack of surveillance. They seek privacy – an ability to be authentic with their truth without being monitored. At home, Winston seeks a private

corner where he can write – a tiny space where he is unobservable and unrecorded. For Winston, personal space is a fundamental requirement for privacy. Henry Giroux observes that the loss of personal space and privacy in Oceania enables the ruling party to commit moral crimes[5] not just political ones ("Totalitarian Paranoia" 109). Igo concurs that *Nineteen Eighty-Four* substantiates the vulnerability of the human mind to external molding (122).[6]

6.2 – Brief Overview of Privacy in the USA

Comparison between Orwell's Big Brother and contemporary surveillance impedes the topic's dissection in public discourse, says Velden (185). In order to show that privacy and mass surveillance are not new categories in the digital age, this research will briefly examine the history of privacy in the USA. This is not a comprehensive account, but rather an overview of the history of privacy initiatives. The difference between privacy and secrecy, or seclusion and anonymity will not be addressed. This section will focus on the relationship of privacy to society.

Western societies have a centuries-long history of fighting against totalitarianism. Desai traced communication privacy in the United States back to the forming of the American post office. The establishment of the constitutional post in the late 18th century was designed to protect the privacy of correspondence and was used by American rebels against the British control. Thus, the guarantee of private communication was an integral part of the fight for liberty (Desai 564).

6.2.1 – Modern Conception of Privacy

Sarah Igo defines three stages of privacy development in the United States. The first one occurs in the late 19th century when technologies disrupted the mentality of the Victorian era. The second stage begins in the early 20th century with the passing of the Social Security Act of 1935. Government was tasked with gathering massive amounts of citizen data to implement the program. The third stage occurs in the 1960s and 1970s marking the transition from the association of privacy with property to focusing on

5 Moral crimes in *Nineteen Eighty-Four* are numerous. The first one that Winston commits is starting a diary. He contemplates the punishment for such an offense being twenty-five years in a forced-labor camp or simply death (Orwell, *Nineteen Eighty-Four* 6).

6 The third act of *Nineteen Eighty-Four* describes in detail the psychological manipulation Winston is subjected to. The result of which is his complete surrender – "He loved Big Brother" (Orwell 298).

identity and psychological freedom (Igo 14). In the US British colonies, privacy was exclusive to the white, male landowner. In the first stage, privacy was guaranteed by "property rights" (Igo 20) and related to the corresponding environment (house, plantation) of the white male.

Even after the 14th Amendment passed in 1868, guaranteeing African-American equality, privacy was still the domain of the white man (Igo 23). Family was the foundation for moral social norms (Igo 22), because management of personal affairs was considered the ultimate expression of masculine control (Igo 23). New technologies of the late 19th century – film cameras, telephone, the telegraph, sound recording and the rise of the yellow press – expanded circulation of personal information. The exponential growth in connections between people allowed for recognition outside the family and circle of friends (Igo 17). As a result, these technologies heightened the issue of individuals' privacy (Igo 17). Therefore, the foundation of the second stage changes from property to personality (Igo 24). In 1890, the lawyers Samuel Warren and Louis Brandeis published their essay "The Right to Privacy" in the Harvard Law Review which created the privacy chapter in the US jurisdiction (Igo 34,35, Perinan 185). This essay addressed damage to reputation caused by unwanted publicity and the resulting psychological harm (Igo 37).

The threat of a World War in the first part of the 20th century escalated surveillance and showed that privacy can be brutally invaded all in the name of patriotism (Igo 48). Surveillance amplified toward German-Americans, immigrants, individuals dissenting from the political course and African-Americans who were considered easy to influence (Igo 49). Fingerprinting was introduced in 1890 and was used to document immigrants, African-Americans, sex trade workers and people from the lower classes (Igo 50). At the beginning of the 20th century, privacy was still only accessible to the middle and upper classes (Igo 50). Individual privacy was slowly evaporating with the emergence of insurance companies, bank and loan offices and various public city departments collecting more information (Igo 45). Passports were introduced around World War I to all social classes (Igo 62), thereby reducing methods of patrol at the border by appearance and bias (Hong IV).

According to Igo, the notion of privacy was altered due to the Social Security Act of 1935 requiring all citizens to register (56). Privacy arrived to public debate as social security numbers were recognized as a form of tracking. The Social Security

Administration became the first big data bank (Igo 72). The mandate was registering and documenting the private details of all citizens for identification purposes (Igo 59). Consequently, private business began to require that current and potential employees submit extensive personal information (in some cases prior to 1935) (Igo 76). At the same time, citizen surveillance concerns shifted from government to private companies (Igo 76,77). By the mid 1940s, some people tattooed their social security numbers acting as personal bar codes, which demonstrated that individuals were accepting the era of "documented identities" (Igo 97). During the Cold War a myriad of privacy attacks were launched by employers, corporations, schools and insurance agencies which Myron Brenton referred to as the Civilian Big Brother (qtd. in Igo 101). This period, says Sarah Igo, blurred the boundary between personal and social life (101). Psychoanalysis was gaining popularity, shifting interest from an individual's external image to focus on their image of mentality and reasoning (Igo 102). Psychologists and counselors praised the mental health of people, equating it to the basis for a healthy democracy. By the 1960s, surveillance of individuals' inner selves was a widely accepted model for "market research, personality test, … opinion polling, subliminal suggestion, truth drugs" (Igo 108).

The third stage occurred in the 1960's with usage of invasive personality tests. Sixty percent of companies collected a plethora of personal information (Igo 135,136). Job applicants were expected to provide details such as political affiliation, union membership, sexual practices, health and social status (Igo 137). Job seekers never knew the results of the test or the impact it had on their employment (Igo 138). Sarah Igo explains this privacy attack on individuals was conducted in every arena of society – "government and the military, corporations and workplaces, universities and hospitals, media and marketers" (142). Marketers further used media manipulation for the sole purpose of selling more products (Igo 123). Psychological data was used for "psychological exploitation" (Igo 127) not only impacting individuals' privacy but also their psychological stability (Igo 128). These universal methods of gathering information combined with media manipulation for mind altering technique were used in the USSR as well (Igo 123), showing American and Soviet surveillance systems were comparable (Igo 104,143).

6.3 – Privacy, Surveillance and Society

This brief account of privacy history shows that the concepts of privacy and surveillance are intimately related, and acquisition of personal information is not a new condition due to digital technology. Rather, the digitalization of contemporary societies accelerated the importance of privacy due to it's inherent fragility (Perinan 185). Karyda et al. concludes that in digital environments, especially when user devices are small or the software unknown, control of the personal information transmitted is extremely limited (204). The scholars find privacy is "one of the basic freedoms of people and the protection of privacy is a social responsibility" (Karyda et al.206). Hollander affirms "There can never be too much privacy" (9) and he places the right of the individual to have secrets as primary to the right of privacy (19). Scholars Priscilla Regan, Alan Westin, Valerie Steeves and Ian Kerr all recognize the social benefits of privacy (qtd. in Friedewald et al. 2). Goold argues that the equalization of power between individual and government is ensured with privacy of thought and feelings (qtd. in Friedewald et al. 5). Friedewald et al. further elaborate that surveillance in public spaces not only diminishes the feeling of living in a democratic society, but also discourages protests and freedom of assembly (5).

Privacy research in the social realm is abundant – Hirshleifer finds that privacy contains a "social structure" (649), Solove echoes this by saying privacy "is a form of freedom built into the social structure" (qtd. in Karyda et al. 196), Dumortier and Goemans find the right to privacy as a cornerstone of democracy (qtd. in Karyda et al. 196) and Tugendhat equates privacy to freedom (qtd. in Perinan 184).

6.4 – Audio Beacon Technologies and the Invasion of Privacy

Examining audio beacon technologies, Mavroudis et al. found that the data gathered is used to create user profiles. The researchers describe six ultrasonic sound security risks and show how user data can be compromised. The findings were "devastating violations of the user's privacy" (Mavroudis et al. 96), because companies were consolidating audio beacon technologies with already developed tracking technologies (Mavroudis et al. 96). The researchers also established "information leakage" (Mavroudis et al. 96), which can be initiated not only by the company, but can be exploited by third parties – employers, hackers and other private or government organizations. Mavroudis et al. discovered the audio beacons manufactured by

Silverpush contained security risks which could harm consumers. Brent Carrara and Carlisle Adams, Do et al. and Sun et al. additionally report audio beacon technologies can be used as a covert way of extracting data from devices (qtd. in Zeppelzauer 1250). Bugeja, Jacobson and Davidsson additionally find audio is among the most invasive technology in the home (qtd. in Lutz and Newlands 147,148). According to Lutz and Newlands audio data is compounded with data from other sources resulting in a "fine-grained user profile" (149,150).

Helen Nissenbaum's theory of privacy as contextual integrity is based on the separation of information within different social environments – physician's office, place of employment, place of worship, educational institution, family circle or commercial enterprise (qtd. in Rubinstein and Good 1372). In these dissimilar places individuals behave differently based on social norms, they embody different functions and they expect the information to remain inside that environment only. Thus restriction of sharing information is based on contextual integrity (qtd. in Rubinstein and Good 1373) and this integrity breaks down when information is linked or shared between different environments. She further distinguishes two separate information streams. First is appropriateness and is related to the type of personal information shared in a given social environment. The second one is distribution, related to whom particular information is shared within a given circumstance (qtd. in Rubinstein and Good 1373).

In the first part of the 21st century, mobile devices have become an integral part of the individual. We carry them to the doctor's office, school, work, driving, shopping, eating and relaxing. As such, audio beacon technologies are pervasive in our lives. In this context, audio beacons infringe upon the contextual integrity of information sharing which undermines users' privacy. Further, audio beacons allow transmission of users' data from private homes – a sanctuary for many and a place that has long been regarded as a surveillance-free environment. This data transmission is not limited to targeted users, therefore audio beacon technologies enable surveillance of law-abiding citizens. As Quentin Skinner, leading British historian of political thought, explains, the actual existence of arbitrary power able to surveil and invade our privacy is an abuse of liberty (Skinner).

CHAPTER 7 – SURVEILLANCE SOCIETIES AND SOCIETAL ORDER

We have explored the contemporary formulation and evolving concept of privacy. To show that surveillance processes and methods of control are not isolated only to the United States, we are going to turn to Michel Foucault's *Discipline and Punish*. In Foucault, we are going to learn the evolution of surveillance and the consecutive development of control systems from society to society. Michel Foucault and Gilles Deleuze describe how privacy, control and surveillance are not isolated for specific societies, but also travel across cultures. The exploration of societal structures in the last two centuries as seen from the perspective of these two scholars clearly echoes privacy operations explored in the previous chapter. This chapter will conclude with the study of the societal order in Orwell's *Nineteen Eighty-Four* and its mode of supervision, which is reversely connected to Foucault.

7.1 – Societal Order in the 18th and 19th Centuries

According to Foucault, public displays of capital punishment enforced the law and the power of the political regime (*Discipline* 47,49,55). He observes that "punishment as a spectacle" (Foucault, *Discipline* 8) slowly vanishes by the beginning of the 19th century and is replaced by trials and sentencing. Thus, the emphasis is placed not on the severity or brutality of the punishment, but rather on the assurance that the criminal will be caught (Foucault, *Discipline* 9). The body is still punished, not by public torture, but by loss of liberties – "punishment that acts in depth on the heart, the thoughts, the will, the inclinations" (Foucault, *Discipline* 16). Therefore, Foucault finds that punishment changes its focus from the body to punishing the soul (*Discipline* 16). This does not eliminate body penalties, rather it builds upon it – "even when they do not make use of violent or bloody punishment … it is always the body that is at issue" (Foucault, *Discipline* 25).

Gilles Deleuze applies the work of Michel Foucault in his historical survey of the features of the control society and the metamorphosis of that control over the years. Gradually, from the 18th through the early 20th century, the *societies of sovereignty* transition to *disciplinary societies* (Deleuze 3*)*, in which the method of control shifts to incorporating buildings to serve as confinements – schools, hospitals, military barracks, factories, and prisons. People are placed in these confined spaces to maximize

efficiency, profits, and eliminate wasted time and space, thereby ensuring a cohesive mass-produced environment (Deleuze 3). For Foucault, these societies are controlling the individual by keeping the body efficient, making it more productive (*Discipline* 26), in a word, creating a *docile body* (*Discipline* 136). The disciplinary societies of the 18th century incorporate documentation to classify, identify and organize these separate docile bodies (Foucault, *Discipline* 148).

Foucault finds another integral aspect to the disciplinary power structure – surveillance. Surveillance monitors production inside the given environment, but more importantly is a hierarchic network (Foucault, *Discipline* 175,177). In a sovereign society, the ruler is visible and exhibits detailed documentation of his deeds as an "account of his life" (Foucault, *Discipline* 191). Documentation of his look, description of his mannerisms and the written record of his daily activities is a privilege bestowed on the worthy (Foucault, *Discipline* 191). Disciplinary societies not only reverse this trend, they adjust the meaning of visibility by turning it into "means of control and a method of domination" (Foucault, *Discipline* 191). In disciplinary society, power structures remain unseen, while people have to be constantly visible. In addition, the person's individuality must be uncovered, because that knowledge guarantees their subordination and objectification (Foucault, *Discipline* 193). Foucault concludes that *discipline* is an intricate system comprised of various techniques and mechanisms that identify *discipline* as power (*Discipline* 215). As such, in the disciplinary society, there is a preoccupation with the organization, classification and normalization of the populace executed with the aid of documentation and "statistical methods" (Cohen 185). Records were "both a technique of power and a procedure of knowledge" (Foucault, *Discipline* 148) which produced individuals "as objects and as instruments" (Foucault, *Discipline* 170). The production of norms, which necessitates the individual's proper behavior becomes the main goal (Galic et al.16, 17).

7.2 – Societies of Control

Deleuze observes that the *disciplinary societies* transitioned to *societies of control* by the mid 20th century (3-4). If large buildings (schools, hospitals, military barracks, factories and prisons) are characteristic of the *disciplinary society*, then the corporation is the embodiment of the *societies of control* (Deleuze 4). In societies of control, Deleuze finds the individual has become a *dividual* – a digital representation of a

person. A *dividual* is the accumulation of digital traces resembling a person, not an individual of flesh and blood. Thus, the interest shifts from the physical body to the online behavior and resulting digital traces. These are combined later in separate settings to form what Haggerty and Ericson call *data doubles* (606). The *data doubles* are examined in different environments (governmental, financial and health institutions) to devise procedures of control, so the data doubles are an "additional self" (Galic et al. 22). Haggerty and Ericson see that the formation of virtual data doubles yield two additional features: the combination of digital traces offer increased understanding interpreting the individual (611) and multiplies the strength of the surveillance (610).

The researchers coin the term *surveillance assemblage* to represent the combination of various data streams that work together when assembled (Haggerty and Ericson 608). Deleuze and Guattari see these *surveillance assemblages* are state designed to specifically capture the flow of data (qtd. in Haggerty and Ericson 608). Haggerty and Ericson reiterate that systems are reliant on technologies to execute the surveillance. The prime motive is to gather large amounts of data to intimately understand the subject. After the information is received, it is reassembled in multiple institutions. The data doubles are investigated and a plan is implemented for control or intervention (Haggerty and Ericson 613). In that sense, Haggerty and Ericson agree that surveillance assemblage is closely connected to Orwell's portrayal in *Nineteen Eighty-Four* and more dissimilar to Foucault's panopticon (612). As an example of this, I suggest, when detailed information about Winston's life, collected over the span of seven years was dissected by those in power, he was captured and punished (Orwell, *Nineteen Eighty-Four* 244).

7.3 – Social Order in *Nineteen Eighty-Four*

In Orwell's portrayal of surveillance, the proles are exempt from the eye of the state. Haggerty and Ericson rightfully observe the disparity between Orwell and contemporary society which surveils everyone (607). I can accept this statement with a caveat. The proles' neighborhood is depicted as a surveillance-free zone where a person can express their true feelings through Winston's description only. We can assume Julia perceives it the same way, because she wanders there as well. However, they are mistaken as we can see from their demise. It appears this is artificially fabricated by the state. The motive being to set a trap to capture hidden dissidents, as it did in the case of

Winston and Julia. More importantly, this is also the neighborhood where Mr. Charrington, a supervisor of the Thought Police, resides (Orwell, *Nineteen Eighty-Four* 224). For Foucault, hierarchical supervision and it's accompanying surveillance apparatus is an integral part of the power structure – "this enables the disciplinary power to be both absolutely indiscreet, since it is everywhere … and absolutely 'discreet', for it functions permanently and largely in silence" (*Discipline* 177). This description can be applied verbatim to the surveillance model en masse in Oceania and directly to the first member of the Thought Police that we meet in the book, Mr. Charrington. According to Foucault, supervision is a vital part of the disciplinary surveillance paradigm – "supervisors, perpetually supervised" (*Discipline* 177).

The supervision and surveillance is conducted by technologies – most widely, telescreens and microphones. The ruling party is attempting to see, hear and catalogue most of the actions of its citizens. In modern societies, we regard the denial of the capacity not to be seen or heard as an infringement of individual rights. However, this situation is reversed in Orwell's book. In Oceania, turning off the telescreen for brief periods is limited to upper members of the party (Orwell, *Nineteen Eighty-Four* 169). It is a privilege that only the powerful have. Despite the modern expectation of privacy, the situation in Oceania resonates today, where a majority of individuals are visible and unable to disappear, as Haggerty and Ericson described it.

7.4 – Audio Beacons Role in the Societies of Control

Roger Clarke coins the term *dataveillance* to represent surveillance by accumulation and use of personal data, in contradiction to surveillance by direct observation (qtd. in Bennett 14). Audio beacons evade this classification, because they collect personal data by direct observation indirectly. Meaning, the information collected and transmitted can directly identify a person, their surroundings and others in the vicinity, while simultaneously collecting data indirectly, because the subject is unaware it's happening. Location tracking and de-anonymization of audio beacon technologies enable a state of full visibility, which contributes to the power imbalance. This environment resembles societies of control where supervision and control are implemented by digital devices. The ability of audio beacon technologies to locate and broadcast the position of any user at any time resembles surveillance akin to an "electronic collar" (Deleuze 7). This digital collar surpasses previous surveillance

technologies through mass transmission of audio data thus allowing large scale surveillance.

The course of events leading to a Big Brother society is not necessary and thus, will not materialize, believes Clarke (qtd. in Bennett 14). Conversely, Deleuze argues that previous methods of disciplinary control have not disappeared or been replaced. Rather, they have been imbued with a more precise, moldable and opaque mode of surveillance and judgement (Deleuze 7). This accumulative societal surveillance paradigm shows that the Big Brother scenario is possible and audio beacon technologies contribute to it through the capture and transmitting of the most intimate and unique traits of an individual (Perinan 184). Galic et al. further observe a relationship between the effortless tracking of individuals (and dataveillance) being linked with profiling and social sorting of people (28).

Bauman argues that marketing principles, not disciplinary actions, govern the surveillance practices of corporations and organizations (qtd. in Haggerty and Ericson 615). Inversely, Haggerty and Ericson argue that data has more than one purpose (619). I agree with Haggerty and Ericson that personal data can be used for more than one purpose. Audio beacon technologies might have been developed with marketing purpose in mind, but the data gathered can be distributed to multiple organizations and thus have numerous uses. We are looking at technologies as extensions of self, but software rights are owned by companies that employ agreements to protect it (the privacy policy's aspect will be discussed in Chapter 9). Audio beacon technologies act as an extension to the software, but companies producing them see individuals as extensions to the technology. This statement and its clarification and expansion leads us to the next chapter.

CHAPTER 8 – BUSINESS AS USUAL

To paint a holistic picture of surveillance and the privacy paradigm in western societies, we need to look at economic implications. Contemporary societies are largely based on economic growth and market share. This overview will help us perceive the economic model and business practices of Google. This research focuses on Google, because the three developers of audio beacon technologies (Lisnr, Silverpush and Shopkick) use Google cookies for their functionality. To establish a general understanding, we will use Shoshana Zuboff's book, *The Age of Surveillance Capitalism*, which encapsulates the previous ideas. The connection to Orwell's book will be analyzed through Zuboff's concept of Big Other.

8.1 – Audio Beacon Technologies and Google Cookies

Zuboff explores the explosive growth of tech giants – Apple, Google, Facebook and Microsoft. For the purpose of this thesis we are going to look at Zuboff's main example – Google. This choice is motivated by the three audio beacon companies, Lisnr, Shopkick and Silverpush which all use Google cookies for delivering their services.

Millett, Friedman and Felten argue that invention of the cookie[7] technologies has always aspired to surveillance since its inception. Researchers state that users had little control over the original cookies installed in the Netscape Navigator 1.1 browser. The user was not notified of cookies so they could not be blocked. A panel for preference modification was absent so cross-site tracking of the user was possible (qtd. in West 27,28). Thus, the foundations of this surveillance network was the marriage of cookie technologies and commercialism as a desirous new business model (West 28). Conclusively, from its infancy the internet was prone to surveillance enterprises and related to the previous social systems centered on manipulation, organization and control of the individual. Audio beacon technologies continue this process by allowing users to be de-anonymized and identified across multiple devices.

One clarification is mandatory at this junction. As Zuboff explores in her book *The Age of Surveillance Capitalism*, the power system described above is enabled by digital technologies, but is not equivalent to them (15). She observes, technologies can be

7 Cookies are data text files stored on the user's computer to facilitate computer identification (Kaspersky)

designed without the surveillance tracking aspect in them (Zuboff, *Surveillance Capitalism* 15). The pervasiveness of surveillance is driven by the monetization of Big Data made possible by digital technologies (Zuboff, *Surveillance Capitalism* 15).

8.2 – Google and Surveillance Capitalism

Google was incorporated in 1998 and even though their search engine was highly regarded, it did not generate a return on investment (Zuboff, *Surveillance Capitalism* 71). The burst of the dot-com craze in 2000 intensified the situation (Zuboff, *Surveillance Capitalism* 72), which in turn prompted Google to administer AdWords – an algorithm that learns from the behavior of its users – "number and pattern of search terms, how a query is phrased, spelling, punctuation, dwell times, click patterns, and location" (Zuboff, *Surveillance Capitalism* 67). This process of aggregating and analyzing apparently worthless information gave birth to target advertising (Zuboff, *Surveillance Capitalism* 65) – showing a particular ad to a particular individual at a precise time when the individual is mostly likely to make a purchase. The invention of target advertising made the company extremely profitable (Zuboff, *Surveillance Capitalism* 67) and introduced predictive algorithms (Zuboff, *Surveillance Capitalism* 68). The data generated serves as the base for creating big data patterns, which feed an algorithm designed to predict users' future behavior. Heerden et al. elaborate that other companies are implementing the same model of data collection from all accessible sources. Moreover, modest storage costs allow companies to collect data even if an algorithm does not exist for analysis with the hope that the future will provide the infrastructure to do so (Zuboff, *Surveillance Capitalism* 3).

According to Zuboff, Google's business model capitalizes on individual data and behavior by "infer[ing] and deduce[ing] the thoughts, feelings, intentions, and interests of individuals and groups … irrespective of a person's awareness, knowledge, and consent" (*Surveillance Capitalism* 80,81). Alone, the collection of technological data was not sufficient for Google and they began to aggregate social data as well (Zuboff, *Surveillance Capitalism* 79). This pioneering model had an additional aspect – taking away the right of the user to decide what data can be revealed (Zuboff, *Surveillance Capitalism* 90). The information flows in one direction only – away from the individuals and toward the data aggregators. This model 1) elevates the buyers of the Big Data to

become the real customers 2) the aggregation and accumulation of users' input breeds an uneven and hierarchic power structure (Zuboff, *Surveillance Capitalism* 94).

Zuboff coins the term *surveillance capitalism*, a system which ubiquitously exploits human experiences by trading their personal data including predictions of future behavior (*Surveillance Capitalism* 8,9). The product generated under surveillance capitalism is personal data. Therefore, individuals and their behavior serve as the raw material, which Zuboff calls behavior surplus (*Surveillance Capitalism* 84).[8]
She sees Google as the inventor of surveillance capitalism (Zuboff, *Surveillance Capitalism* 9)[9] with their creation of target advertising (Zuboff, *Surveillance Capitalism* 65). In addition, this instrumental power yields the possibility of manipulating users' actions, a possibility further confirmed by the public leak of Google's "Selfish Ledger" (Heerden et al. 7). With its infinite storage of data, predictive and behavior changing capabilities, surveillance capitalism threatens individual independence, freedom of choice and ultimately democracy (Zuboff, *Surveillance Capitalism* 54). Zuboff calls this economic model "Faustian" (*Surveillance Capitalism* 11) because users are trapped inside the global internet system and are incapable of severing the connection. Simultaneously, the system has the capability to ruin them.

8.3 – The Old is New

Facebook further developed surveillance capitalism. The social platform not only utilized behavior surplus to meet demand, they devised a model to generate more demand (Zuboff, *Surveillance Capitalism* 92). This was largely accomplished by hiring Google executive Sheryl Sandberg as Facebook's COO in 2008 (Zuboff, *Surveillance Capitalism* 92). Zuboff calls the rise of Google and Facebook the "third modernity" (*Surveillance Capitalism* 46). This stage is characterized by the creation of the verbose online privacy policy. This lengthy document discourages meaningful user participation

8 The idea of surplus value can be traced back to Marx. Stephen Resnick states that Marx sees one of the pillars of capitalist society to be the idea of surplus value. Workers are producing value by working, but they are paid less than the value they produce. This difference is called surplus value (Resnick 00:03:25-00:05:17).

9 Surveillance Capitalism is described by Zuboff as "a new economic order that claims human experiences as free raw material for hidden commercial practices of extraction, prediction, and sales" (*Surveillance Capitalism*, The Definition).

(Hoback 00:04:13-00:04:29) and ensures the course of surveillance capitalism with a simple quasi-voluntary click (Zuboff, *Surveillance Capitalism* 48)[10].

Surveillance Capitalism is not a new trend and Zuboff alludes to the historical struggle for power and domination in the beginning of her book (*Surveillance Capitalism* 3). However, this point is better explored by the tech scholar Evgeny Morozov, who criticizes Zuboff's view. Morozov points out how surveillance capitalism is a continuation of 19th century capitalism. He believes it to be a continuation of the "managerial capitalism" of the big business companies (Morozov IV, V). Josh Lauer also finds that contemporary surveillance practices were developed in the 19th century, with the development of the business credit score (qtd. in West 25). Lauer confirms Igo's observation that technologies were created to interpret the data extracted from surveys in the mid 20th century which expanded the collection of personal data from credit card transactions and phone calls for marketing purposes (qtd. in West 25).

8.4 – Economic Repercussions

Marozov points out that surveillance capitalism also generates value, an observation that is missing from Zuboff's book (XII). This point is further supported by the research done by Goldfarb and Tucker. They measure the effect of online advertisements before and after the enactment of data privacy laws in Europe. The researchers found that in Europe, once the Privacy Directive laws were implemented, the effectiveness of the ads declined by 65%[11]. The economic inference from limitations on massive data collection is that companies have to spend more money on advertising to achieve the same results. Goldfarb and Tucker conclude, however, that the added expenditure is only one side of the coin. The increase cost to advertisers must be weighed against consumer privacy (Goldfarb and Tucker 70). John Havens, in his book *Heartificial Intelligence,* shows the triviality of the market system based on gross domestic product and advertisement. According to him, the science of positive psychology shows that individual happiness is not related to buying more goods (Havens XXVI).

---

10 Privacy policies, the language they carry and it's implications will be discussed in Chapter 9

11 Goldfarb and Tucker acknowledge two conditions – 1) there are disparities between clicking on an ad and actually purchasing a product and 2) they show that only 26% of people see online ads (62).

A succinct paper by Richard Posner examines “concealment of information” (405) from an economic perspective. The author correlates privacy and non-disclosure of personal information with fraud (Posner 406). To him “’selling’ oneself and selling a product” (Posner 406) is equal, therefore, not disclosing personal details to your employer (potential or current) is harming the corporation and the economy (Posner 405). To Posner, privacy leads to more unemployment, lower wages and higher interest rates (407). Posner identifies the leading advocates and beneficiaries of increased privacy are people with “more arrests or convictions” (407). To him these people “overlap strongly with racial and ethnic groups, namely black and Hispanic Americans” (Posner 407). Posner concludes that increasing privacy will have dire consequences, which is to be avoided at all costs, namely – “a redistribution of wealth from whites to members of these racial and ethnic groups may result” (407).

8.5 – Market Economy

Zuboff’s surveillance capitalism is based on consumers the same way Marx capitalism is based on labor – if you remove the consumer (or labor) the system fails (Marozov XII). Zuboff talks about behavior surplus, but the idea of surplus value can be traced back to Marx. Marxist economist David Harvey observes money can take many different forms (“Part 3” 00:58:50-01:00:13, 01:26:30-01:27:49), so in the digital society, money has another form – invisible binary bits of code. In such societies, from a corporate perspective, the implementation of digital technologies reduces labor, which in turn increases surplus value and profits. This point is supported by the amount of employees and the revenue of the companies. In 2014, the top three Big Tech companies had 137,000 employees and $247 billion in revenue. Compared to the late 1990’s, the top three automakers had $250 billion in revenue and 1.2 million employees (Zuboff, “Big Other” 80). Another way to increase surplus value and subsequent profits in digital societies is to generate more data, which in pre-digital societies would have been done by increased working hours. Today, this is achieved by encouraging users to use more devices, to connect these devices and thus to generate continuous data. Audio beacon technologies, with their location and cross-device tracking, and de-anonymization capabilities are also major factors in this process of generating continuous data, and thus increasing surplus value.

In the perfect market, as described by Adam Smith, no one person can command the price because the market does that collectively (Harvey, “Part 3” 00:03:10-00:16:50). However, Smith observes that the perfect market dictates perfectly informed parties (Smith). As observed by Sarah West, companies are notorious for hiding their modes of collecting data and their business transactions connected with the use of that data (37). This creates an immense information imbalance. The promotion of transparency “as inherent good” (West 37) is misleading, because users are the only ones that are sharing their data, where companies are not transparent about their business practices. So consumers are not sentient participants in the collectivity of the market.

8.6 – The Big Other

Zuboff notes the difference in surveillance capitalism from previous capitalistic models is the disconnect from the need of human bodies for the business to operate (“Big Other” 80). The generation of data or the commodity does not necessitate employees, because extraction of human behavior data is a default condition of the way the technology is set up. This unprecedented freedom is a break from previous capitalistic systems (Zuboff, “Big Other” 80). Zuboff names this new regime of accumulation and commodification of all daily experiences, thoughts and actions the *Big Other* (“Big Other” 81). To her, the Big Brother term is not appropriate any more because power can not be centralized, but at the same time there is literally “no escape from Big Other” (Zuboff, “Big Other” 82). Zuboff finds that public unawareness of the business practices of Big Tech surveillance capitalism to be its main enabling condition. This lack of public knowledge about how surveillance capitalism works is the main source of its power (Zuboff, “Big Other” 83) – “democracy threatens surveillance revenues” (Zuboff, “Big Other” 86) and Henry Giroux agrees “secrecy is a virtue for which there is no democratic accountability” (“Totalitarian Paranoia” 122,123). So, the importance of Zuboff’s argument is that surveillance capitalism is dangerous to democracy (Galic et al. 25), especially in the USA where the Bush and Obama administrations have passed legislation by virtue of which “State governance has been freed from the rule of law” (Giroux, “Totalitarian Paranoia” 124).

8.7 – Audio Beacon Technologies, Business and Implications

To address the socio-economic implications related to the implementation of audio beacon technologies, let us now explore their active realization in applications that are widely used in our digital society. The research by Arp et al. and the discussion in Chapter 4 focused on three companies developing those technologies – Lisnr, Shopkick and Silverpush.

The Cincinnati-based start-up, Lisnr, has been partners with VISA since 2015 and recently the credit card giant has invested more capital in the company (Butler). In addition to VISA, Lisnr has partnered with Ticketmaster for processing ticket scanning and transacting payments, and cell phone authentication (Butler). Lisnr has also partnered with the music band Swedish House Mafia, singer J. Cole and Budweiser Made in America tour and are collaborators with Jay-Z's record label (Flynn). In all these situations, Lisnr is using their algorithm for transactions based on audio, but that function does not replace the capabilities discussed in Chapter 4 – location tracking, de-anonymization and cross-device identification. Case in point is the fact that Lisnr has also partnered with Jaguar Land Rover for customization of automobile settings (Rehbock). Lisnr claims that they can determine and differentiate who the driver of the vehicle is and who the passenger is (Rehbock). Additional partners that Lisnr is working with are listed on the company's website and include – Intel, Synchrony, MIO and SAP (Lisnr, "Trust").

The second audio beacon development company listed, Shopkick, is venturing into the retail market. They are working with retailers such as American Eagle, Sports Authority, (Slade) Macy's, Target (Forbes) and ExxonMobile (CSP). In addition, Wal-Mart, Virgin Atlantic and Duane Reade are all considering implementing the Shopkick technology (Slade). Further clients are listed on the company's website – 3M, Duracell, The Home Depot, Best Buy, Coca Cola, H&M, L'Oreal, P&G, TJ Maxx, Marshalls, Sam's Club and Nestle (Shopkick, "Become a Partner").

The third developer of audio beacon technologies, Silverpush, has recently partnered with the marketing firm Digital Commons, in New Zealand, to be implemented in videos (Silverpush, "Partners"). This will result in tracking individuals' TV viewing habits.

As seen from this exhaustive list, the clients of audio beacon technologies range from retail, to automotive, to banks, tech companies, airlines, and many other industries.

The rising trend of incorporating these invasive technologies is alarming, especially when we take into consideration their opaque surveillance faculty. Several studies by Martinez-Martin, Insel, Dagum, Greely, and Cho, identify the rising prominence of small sensors in the collection of data for identification of human behavior (qtd. in Heerden et al. 2). Purtova observes that the accumulation of data leads to another imminent danger – the de-anonymization of that data revealing the identity of the individuals to which the data belongs (qtd. in Heerden et al. 2). As such, audio beacon technologies are becoming an integral part of an emerging web of surveillance and permit the elimination of previous targeted surveillance practices. The mass scale surveillance and transmission of data afforded by audio beacons are contributing to an unbalanced power paradigm in capitalist economy. Zuboff defines the business practices of Google to be collecting all data possible with disregard for privacy until “resistance is encountered” (“Big Other” 78). Since the above-mentioned developers of audio beacon techniques are using Google cookies, I would argue that their business model would be the same.

Venier and Mordini address soft biometric (speech and voice identification) technologies and their privacy implications. The researchers argue that these auditory technologies can be used not only for identification but also for *categorization* of people. Audio surveillance technologies, because they are covert, can be used habitually to aggregate personal data and to map out individual behavior. According to Venier and Mordini, this can lead to generating classification of normal and abnormal behavior (qtd. in Friedewald et al. 16). Friedewald et al. further observe that audio surveillance can be used for automated surveillance on desired topics as well as particular individuals (17). The researchers agree with Venier and Mordini, that the danger is not identification of individuals, but rather their categorization (17). Once the data is aggregated and analyzed, it becomes an essential component of the individual and the digital profile becomes the foundation for future judgements (Friedewald et al. 17,20).

Harvey observes that the state conceptualizes people by their names and bodies (“Part 1” 00:56:45-00:58:25). In other words, the state views people as things. He argues that this conceptualization model does not match with the actual life of the individual, because living life is a process (Harvey, “Part 1” 00:56:45-00:58:25). In that sense, it matters if we continue to generate data, because the processes of the continuous generation of data helps conceptualize humans as dividuals, where a person is the sum of their digital traces and not an individual of flesh and blood.

Henry Giroux observes the infiltration and normalization of surveillance into everyday life. With the normalization however, another aspect appears – the *regime* of surveillance (Giroux, “Totalitarian Paranoia” 113). This regime is in stark contrast with the values of modernity such as “emphasis on enlightenment, reason and the ideals on justice, equality, freedom and democracy – however flawed” (Giroux,“Totalitarian Paranoia” 114). Contemporary neoliberal capitalism undermines those ideals for the expense of the collective enterprise of business and security, driven by the dollar sign (Giroux, “Totalitarian Paranoia” 115,117). To Giroux, the most alarming trend of loss of privacy is not the normalization of surveillance, but its luring nature exhibited in social media platforms and the consumer culture (“Totalitarian Paranoia” 111). The appeal of surveillance leads us to the next chapter where we can find the answer to the question – if the encroachment of surveillance into our lives is so oppressive, why do we not resist?

CHAPTER 9 – SELLING THE SOCIAL ORDER

To answer the above stated question, I will begin by addressing four aspects of surveillance in Orwell's *Nineteen Eighty-Four* – 1) the use of language, 2) the dichotomy between surveillance and security 3) changing of the past and 4) entertainment value. This chapter will include a synopsis of Aldous Huxley's *Brave New World* and will explore the comparison between Huxley's and Orwell's books. The juxtaposition will be surveyed through Neil Postman's book *Amusing Ourselves to Death: Public Discourse in the Age of Show Business.* In his book, Postman pins both dystopian visions as opposites. However, this thesis will take a different approach and examine *Nineteen Eighty-Four* and *Brave New World* as complimentary. This method will show a new type of surveillance present in contemporary societies. This surveillance praises the collection of private information, marketed through various channels of popular culture and social media. I call it entertainment surveillance.

9.1 – Language in *Nineteen Eighty-Four*

In 1946, George Orwell wrote the essay *Politics and the English Language*, in which he explores the decline of the English language. According to Orwell, language is a tool that we mold to achieve our objectives (Orwell, *Politics* 2462) and is connected to politics especially when all issues are politicized (Orwell, *Politics* 2569). Therefore, the decline of the English language is not connected to inferior writers, but rather has political and economic reasons (Orwell, *Politics* 2462). Politics is "a mass of lies, evasions, … and schizophrenia" (Orwell, *Politics* 2469), so language has to make "lies sound truthful" (Orwell, *Politics* 2471) by containing "sheer cloudy vagueness" (Orwell, *Politics* 2468). He concludes that an unhealthy social environment hurts language, but the process goes both ways – "if thought corrupts language, language can also corrupt thought" (Orwell, *Politics* 2469). Three years later he implemented those observations in the newly generated language in Oceania called Newspeak.[12]

12 Orwell elaborates on the use of Newspeak and its effects in the Appendix of *Nineteen Eighty-Four*. By popularizing the use of abbreviations and eliminating the use of words, Newspeak "diminishes the range of thought" (Orwell, *Nineteen Eighty-Four* 300). Abbreviations not only squeeze down a word, but also change its meaning by disassociation (Orwell, *Nineteen Eighty-Four* 307). By using Newspeak, a Party member shows their commitment to the Party, but the usage also eliminates external influence (Orwell, *Nineteen Eighty-Four* 299,300). A Party member does not need to know what other options exist, not having alternatives is

Orwell shows how language is used as a tool to confuse individuals, to subdue reasoning and ultimately manipulate public opinion and soften dissent. Examples supporting the above statement are abundant in *Nineteen Eighty-Four.* We will focus on the primary ones – the four Ministries and the Party slogans. The principle by which language becomes a main vehicle of controlling the masses is the inversion of concepts. There are four Ministries in Oceania which monitor and control the entire population. The Ministry of Plenty concerns itself with rations and thus ensures the minimum amount of provisions needed for an individual to survive. The Ministry of Love deals with matters of the law. Since love relationships are eradicated in Oceania, the only contingent for forming a family is based on a matching service administered by the Party. This ministry also punishes dissidents or people committing thoughtcrime[13]. In this case, the love of the Party towards its citizens stems from the idea that the Ministry of Love is helping dissidents to conform to normality. The method of conversion is based on torture, which is administered for the individual's own good. The Ministry of Peace concerns itself with war. By continuously fighting either Eurasia or Eastasia, the Ministry of Peace keeps the adversaries on the periphery of Oceania and thus guarantees a relative peace at home. The Ministry of Truth deals with matters related to the official narrative of Oceania, lies. They alter records to match current situations, thus showing that the Party is always correct. The inversion of meanings is further visible in the three main slogans the party uses to ensure the masses are not veering off the main direction - "War is Peace, Freedom is Slavery, Ignorance is Strength" (Orwell, *Nineteen Eighty-Four* 4).

Orwell explains that changing the language and the elimination of words will eventually lead to a society that does not know the meaning of certain words. The main target is words such as equality and freedom, because these concepts will be "nameless and therefore unimaginable" (Orwell, *Nineteen Eighty-Four* 311).

9.2 – Language in Privacy Policies

In our contemporary surveillance scenario, the most prominent use of language to confuse audiences is evident in the company's privacy policies. "Privacy policies are verbose, difficult to understand, take too long to read, and may be the least-read items

preferable. All they need to know is that Newspeak is the language of the Party and all other languages are faulty (Orwell, *Nineteen Eighty-Four* 306).

13 Thoughtcrime, or the crime of having thoughts against the ruling party, is the leading criminal offense in Oceania and is punished by death (Orwell, *Nineteen Eighty-Four* 28).

on most websites" (Reidenberg et al. 39). They seem designed to dissuade users from reading the text. In *The Age of Surveillance Capitalism,* Zuboff refers to them as "adhe[sive]" (48) because the user does not have an option to use a particular service if they do not agree to the terms. She also refers to them as "click-wrap" (Zuboff, *Surveillance Capitalism* 48) because users agree to them without reading them and as such are bound by them legally.

Reidenberg et al., regards them as the most important information regarding users' privacy (39). Privacy policies are implemented to replace government regulation and as such users need to understand them to make the correct choice (Reidenberg et al. 41,42). However, the average user is usually unaccustomed to the language and the legal terms written in them (Reidenberg et al. 46). Further, the scholars observe that privacy policies are used by the websites to push individuals to reveal more private information than necessary for the transaction (Reidenberg et al. 46).

9.3 – Audio Beacons, Cookies and Privacy Polices

As we examined earlier, audio beacon technologies have been implemented in many different applications. A review of the privacy policies of the three companies scrutinized earlier, Lisnr (Lisnr, "Privacy Policy"), Shopkick (Shopkick, "Privacy Policy") and Silverpush (Silverpush, "Privacy Policy"), reveals two important factors. All three companies use data from third party apps and they share the data with third parties. It is salient that all three companies use Google cookies and are collecting data continuously, in line with Google's business model. Reviewing Google's privacy policy is not an easy task, because it is categorized into eleven different sections (Google). The first sentence initiating Google's privacy policy reads - "When you use our services, you're trusting us with your information" (Google). Downloading their privacy policy reveals that it is thirty pages long, there are numerous embedded links to concepts and further explanations.

A quick comparative look at another application that utilizes audio further shows how companies can use cookies without the need to sell an individual's data. *Signal* is a privacy-oriented communication application that can be installed on any mobile phone. The first two sentences in their privacy policy read - "Signal is designed to never collect or store any sensitive information. Signal messages and calls cannot be accessed by us or other third parties because they are always end-to-end encrypted, private, and secure" (Signal). The following two sections are *minimum age* and *account registration*

and consist of a total of 4 sentences. The subsequent sentence reads – “Signal does not sell, rent or monetize your personal data or content in any way – ever” (Signal). This simplicity and straightforwardness is striking to say the least, but it shows us that companies can structure their business model in a way that does not require them to use their technologies in a surveillance manner. This comparison also shows how cookies can be implemented and individuals’ data gathered without the need to sell it.

9.3.1 – Propaganda

Another term used to describe the use of language as a communication device for influence and misinformation is the word propaganda. Propaganda is intrinsic to any social system. It lures people to embrace an exploitive system masquerading as something which is justified and beneficial.

The following two examples quoted by Zuboff show propaganda in the contemporary surveillance economy. Hal Varian, Chief Economist for Google, sees the barometer for future predictions to be the observation of the rich, because everyone wants to be like them (Zuboff, “Big Other” 84). Rich people have personal assistants therefore, the rest of the people would like to emulate this. He made the above statement in 2014 when he was promoting the use of the voice-activated personal assistant Google One (Zuboff, “Big Other” 84). What Varian does not cover is the fact that digital assistants are nothing like live personal assistants. Google One can not make you a latte or can not take your kids to school. Murray Shanahan, in his book, *The Technological Singularity,* observes that digital assistants “lack a commonsense understanding of solid objects and spatial relations” (55), so despite the marketing rhetoric, as far as functionality goes, digital personal assistants are crippled.

Larry Page, founder and CEO of Google, takes data propaganda to the next level – “In general, having the data present in companies like Google is better than having it in the government … because we obviously care about our reputation” (qtd. in Zuboff, *Surveillance Capitalism* 60). Page is missing a fundamental difference between corporations and government. Governments are institutions concerned with the betterment of society and as such, improve the life of the citizens (Galic et al.19). Corporations are concerned with profits and their loyalty lies with the board of directors and the selected preferred stock holders. Galic et al. go even further to state that corporations do not have “interest in the needs of populations, societies or states” (25).

9.4 – False Dichotomy

Data security expert Bruce Schneier identifies the most widely used argument against privacy today to be its equation of privacy with criminality (qtd. in Solove 2). The dichotomy is presented in the following form – if you have nothing to hide, then you have nothing to fear (Solove 2, 3). Posner similarly formulates it – “Why would someone want to conceal a fact, except to mislead others in transacting with him?” (408).

Woodrow Hartzog points to the structure of the dichotomy and shows that its framing determines the answer to the question (1021). Robert Entman agrees that framing the argument determines the importance of some aspect of the text (qtd. in Hartzog 1024). Daniel Solove concurs that framed as such, the argument shows opposing values to both concepts. Consequently, framed in this way, the value assigned to security is higher than privacy value (Solove 7). The argument stated in the above framework eliminates other options (Hartzog 1026) and implies that privacy need not be defended at all (Hartzog 1026,1027).

Solove states a few additional problems with the above stated dichotomy. One of them is that the privacy-security dichotomy mutually excludes privacy and security, when in reality, security techniques enhance privacy. Solove argues that eliminating privacy does not make society more secure and protecting privacy does not negate security (qtd. in Hartzog 1029). While he argues for privacy, he does not oppose the government’s collection of information with a court order, because this process ensures oversight and necessitates the establishment of probable cause or accountability (Solove 22,23). He suggests that one of the sacrifices of living in a democratic society, as opposed to an authoritarian society, is less than perfect security (qtd. in Hartzog 1030).

Solove additionally finds two other problems. First is the third party doctrine which states that people sharing personal information with a third party should not have privacy expectations (Hartzog 1028). Second is the use of data allows information collected for one purpose to be used for additional and different purposes without the permission of the individual (Solove 19).

The latter characteristic relates to the pervasive data that audio beacon technologies gather. The constant capture of users’ audio in different environments can be used for various purposes. Users are unaware of who the data is shared with or how

the data is used. For example, audio data gathered at the doctor's office, might be used by an insurance company to raise the premiums of the individual.

9.5 – Altering the Past

Giroux observes that reconfiguring society's memory facilitates the growth of surveillance networks. He cites David Price who argues that history is one of the tools we can use to fight misuse of power (qtd. in Giroux, "Totalitarian Paranoia" 128). Giroux finds the expansion of neoliberal politics and the advertisement that emphasizes consumerism and individualism weaken collective memories of unity in the struggle against governmental or private power abuses ("Totalitarian Paranoia" 129).

In Orwell's *Nineteen Eighty-Four,* the relentless and perpetual reshaping of the past extracts from the ruling Party's motto – "Who controls the past controls the future; who controls the present controls the past" (248). By changing the records, the Party eliminates the individual's point of reference and the newly recorded information becomes the truth (Orwell, *Nineteen Eighty-Four* 45). By removing the individual's point of reference, the Party controls the memories of its citizens (Orwell, *Nineteen Eighty-Four* 248), which is their goal. By altering the past, the Party ensures their perceived sense of perfection which eliminates belief there are failings or a need for improvement. Therefore, historical records are signs of weakness and by abolishing them, the Party ensures that "Nothing exists except an endless present in which the Party is always right" (Orwell, *Nineteen Eighty-Four* 155).

This technique of re-writing the past is embraced by tech titan Google. The company records its evolving privacy policy on its official archival page. However, the changes of the privacy policies do not match historical records[14]. Google's original privacy policy from August, 2000, as recorded by the Wayback Machine, is different from the privacy policy stored on Google's site from the same time (Hoback 00:10:16-00:12:01). This altering of the records helps mitigate Google's contemporary business practices, which disregard notions of privacy. Google's erasure of the past privacy policy can be connected with the change in their business model as described by Zuboff in *The Age of Surveillance Capitalism*. She classifies two stages in Google's development since

14 The Wayback Machine is a not-for-profit archival system that records websites through the years. They have been in business since the 1990s, and the way they operate is by taking snapshots of websites and their various pages and log them for public view.

its inception in 1998. The initial stage is characterized by the absence of advertising and the founders dream to design a superior search engine. She calls it “behavioral value reinvestment cycle” (Zuboff, *Surveillance Capitalism* 69) because of the absence of monetization. This stage changed to a “behavioral surplus” (Zuboff, *Surveillance Capitalism* 82) model, identified by the aggregation of data from every single search for fiscal purposes.

9.6 – Perpetual War and the Release of Emotions in Oceania

In Oceania, the Party realizes that emotions could build up in the populace and that a release outlet is needed. This requirement of releasing accumulated rage is met by the *hate week* and its accompanying hate song (Orwell, *Nineteen Eighty-Four* 148). Parades, films, telescreen programs and pamphleteering are all designed to achieve the release of raw emotions. The society of Oceania is based on war. There are two war principles – war against the individual (internal) and war against the foreign enemy (external). The reason entertainment is missing from the world of Oceania is because the society is based on war (external and internal). The war against the foreign entity is in the background and has one leading characteristic – it’s perpetual. When Eurasia is an enemy, Eastasia is an ally and vice versa (Orwell, *Nineteen Eighty-Four* 246). Therefore, the identity of the enemy is not important, the crucial element is that an adversary should always be present. The purposes of this condition are: 1) to keep the members of society in a constant state of anxiety and 2) to establish the Party as an indispensable protector of the citizens from an ever-present danger.

The second principle – the war against the individual, is largely affected through surveillance. The two purposes of the second principal of war are: 1) to hunt down and capture any infiltrators from foreign governments that threaten the existence of Oceania and 2) to identify and capture dissidents within the state.

9.7 – Entertainment Surveillance

Haggerty and Ericson see Orwell’s vision of surveillance in Oceania to be misplaced (606). They state two reasons for it. First, Orwell could not have predicted the rise of the computer and its union with cameras. Second, he did not see the role of private organizations as surveillance enforcers (Haggerty and Ericson 606). Monetizing

the privacy of users, which is what I mean by the section title 'Selling the Social Order,' is largely missing from the world of Oceania.

In contemporary society however, there is a new kind of surveillance. Haggerty and Ericson observe that administrative surveillance is present in all establishments today (618). Private businesses not only normalize the surveillance state, but they are also making it entertaining. If “Orwellian surveillance is somehow patriotic” (qtd. in Giroux, “Totalitarian Paranoia” 121), there is, in contemporary society, a new form of 'entertainment surveillance'. This kind of surveillance glorifies the collection of private information and is popularized by social media, movies and TV shows.

Haggerty and Ericson show how Closed-Circuit TV footage is used for entertainment purposes in TV shows (616), a trend which culminates in the show *Big Brother* where participants are watched 24/7. This mode of entertainment reduces the impact of mass surveillance by turning it to voyeuristic amusement (Giroux, “Totalitarian Paranoia” 113). Entertainment surveillance inverts the previous convention that spying on law-abiding citizens was done for the purpose of national security and is a procedure reserved for authoritarian regimes (Giroux, “Totalitarian Paranoia” 113,114). *Entertainment surveillance* and its accompanying desire for market share and celebrity-seeking status has made surveillance an accepted form of performance (Giroux, “Totalitarian Paranoia” 115). Thus, entertainment surveillance has reduced the loss of privacy from a violation to an annoyance in the course of the individual’s participation in the consumer lifestyle (Giroux, “Totalitarian Paranoia” 111).

Social media also leads to the blurring of boundaries between “watcher and watched” (Galic et al. 27) and the intentional submission to surveillance. Albrechslund calls it “participatory surveillance” (qtd. in Galic et al. 29). Entertainment surveillance is infectious. According to Kristen Boehner, emotions are quantitive and computers can measure them (qtd. in Stark 17), which leads to the findings of Luke Stark that emotions communicated online are “contagious”(14). The spreading of entertainment surveillance can further be assigned to the fact that exposing oneself and watching others online can help an individual with “identity formation” (Galic et al. 23).

Josh Harris, one of the first internet entrepreneurs and the founder of Pseudo – the first internet TV platform that mixed video with chat – observes that Andy Warhol’s view of everybody wanting 15 minutes of fame is missing a key component. Warhol’s quote refers to a person’s lifetime, where Harris believes that people want that attention

on a daily basis (qtd. in Timoner 00:36:48-00:36:59). Therefore, entertainment surveillance has a couple of consequences. First, the daily need for attention reduces individuality to short-lived, narcissistic displays (Giroux, “Totalitarian Paranoia” 112). Second, the complete and voluntary aggregation of all individual activities eliminates the need for the unnecessary exhibition of power, a condition that is necessary in Oceania (Giroux, “Totalitarian Paranoia” 112).

Neil Postman, in his book *Amusing Ourselves to Death: Public Discourse in the age of Show Business,* also addresses the rising importance of visual presentation over content (76). The most important aspects, in the age of visual communication, become marketing products and entertaining audiences (Postman 112,128). All other aspects of culture, which are not adhering to the model, are receding in importance (Postman 90,91). This model further dictates that all topics covered, regardless of significance and harshness, should be displayed in an entertaining manner (Postman 87). The gloss of the image is further enhanced by motion graphics, non-diegetic music, sound effects, and well-composed mise-en-scene. The short format of the message and its framing by lively commercials reminding viewers of a trip to the mall, additionally promotes commercialization (Postman 99,128). According to Postman, the conversion from *news for information* to *news for entertainment* causes disinformation, which nourishes ignorance. But the issues begin when ignorance is mistaken for knowledge (Postman 107,108), because news for entertainment alters important policy debates into a “baby-talk” (Postman 155). To compete and win, politicians market their personalities, not the ideas they want to implement. Therefore, television shapes the outlook of the world, but consequently, the world is arranged for the best television experience.

Jumping a few decades forward, today's entertainment surveillance is characterized by several aspects. It involves innumerable actors-agents present in the social media environment (Scolari 14). This new environment allows its participants to virtually and instantaneously interact with each other through various fan-based sites, blogs or comment sections. Entertainment surveillance enables users to self-market themselves. This often happens through sharing personal content, feelings and situations. The main innovation of entertainment surveillance is target advertising – which is the marketing of goods to users based on their viewing habits. This system involves various algorithms acting as a middle-man between the buyer and the seller. It incorporates different “content providers, affiliate sites, search engines, portals, internet

service providers, software makers" (Carr 46). This mode of advertising provides revenue for countless companies positioned between the viewer and the 'entertaining' content. Entertainment surveillance incorporates various surveillance techniques – eye tracking, auditory surveillance, content viewing, cross-site and cross-device tracking. Audio beacon technologies contribute to the entertainment surveillance paradigm with their capabilities of recording TV audio output and other device content. As a result of the user's choice of entertainment, a personal profile is generated and can be used for commercial purposes and data sharing.

9.8 – Aldous Huxley's *Brave New World*

Aldous Huxley wrote *Brave New World* in 1932 in a social environment exalting technology and science as vehicles for a utopian future (Ball 338). According to Ball, at the time the book was published reviewers were not pleased with the portrayal of a totalitarian state made possible through technological advancement (338). However, those views were altered with the use of the atomic bomb in the Second World War and Huxley's dystopian vision was hailed as a foreshadowing of the negative influence of technology and science on society (Ball 338). The book has been a subject for debates on Foucault's disciplinary societies, "feminism, psychoanalysis and cultural materialism" (Hamamra 12) and discussions regarding science, philosophy, politics and art (Ball 338).

Brave New World is a novel that incorporates multi-personal perspective. The narrative is told through the perspectives of Lenina Crowne, Bernard Marx and in part by John (The Savage). The novel is situated in Central London where individuals' embryos are hatched. This enables the government to pre-determine the intellectual and physical capabilities of all the citizens and pre-classifies human beings into different castes. The society encourages casual sex among its citizens and the family unit is obsolete. Consumerism and escapism are the base of the society and every bad feeling or unpleasant notion is cured by the drug soma. Soma is given to the population for free and by taking the pill, an individual can escape reality by elimination of pain and anxiety. Soma helps the government to control the minds of the individuals. In London, the population is conformed to the governmental standards which contribute to a stable society. In this stable environment, religion, art, creativity and provocative literature are banned and control over the populace is complete because they love their condition.

Lenina agrees to join Bernard on his trip to the Savage Reservation in New Mexico. Visiting the Director to obtain the permits, Bernard learns that the Director had visited the reservation many years ago with a female companion who was lost in a storm. On the reservation Lenina and Bernard are repulsed by the natural process of aging that affects all people. Bernard learns that the Director is planning to send him to Iceland and thus exile him. Simultaneously, Bernard and Lenina meet John and his mother, Linda. Bernard realizes that Linda is the woman that went with the Director and John is their son. Obtaining permission to bring them back to London, Bernard escapes the wrath of the Director, becomes a celebrity and hosts parties in which he introduces John (The Savage). John falls in love with Lenina, but does not understand the promiscuous culture of London where people are encouraged to have sexual intercourse with as multiple partners without the need to fall in love or form a meaningful relationship.

Lenina is equally frustrated with John and does not understand his lack of interest in sex. Several events lead to the downfall of the characters – John refuses to join the dinner parties which in turn eliminates the celebrity status of Bernard and Linda. John's mother dies from taking soma pills consecutively over the span of many days. John, enraged by the situation, attempts an uprising, but instead is arrested with Bernard and his friend, Helmholtz. All three are brought in front of Mustapha Mond, one of the ten world controllers. John and Mond debate the value of social stability versus freedom and choice. Bernard and Helmholtz are exiled to different locations, while John chooses to live in the countryside. Discovered by the citizens he becomes an attraction once again, drawing crowds to see him. Lenina comes as well, but he strikes her with a whip. The situation grows to an extreme and develops into an orgy, in which John partakes. The next morning he realizes that he has surrendered to the ways of the New World and kills himself.

9.9 – *Nineteen Eighty-Four* and *Brave New World*

For Postman, the cultural environment of television entertainment is better reflected in Aldous Huxley's *Brave New World* than in Orwell's *Nineteen Eighty-Four* (141). Postman elaborates that Orwell's vision of the authoritarian state seems to belong to the past, with its simplicity and gaudy display of power (155,156). However, Postman fails to notice that even though the societal order and surveillance in Oceania seems to

be caught in the historical details of his time, the surveillance principles enabling authoritarian regimes have not changed. As examined in this thesis, the surveillance methods have improved and evolved to fit current conditions. Additionally, they have been enhanced with other aspects (entertainment, false dichotomy, self-marketing) to increase their viability. In the context of this research on audio beacon technologies, I have found that both dystopian visions of Huxley and Orwell compliment each other. This thesis will take a different approach than Postman's as it proposes that *Nineteen Eighty-Four* and *Brave New World* can be juxtaposed in a symbiotic relationship to enlarge our understanding of contemporary society.

In Huxley's *Brave New World,* members of society are indifferent to the social paradigm because they are too busy experiencing pleasure (XX). The recipe for happiness in Huxley's world is endless – consumerism aided by a pharmacological compound called soma. In order for the consumeristic social structure to function, the physical environment needs to accommodate individuals by providing countless forms of entertainment – synthetic golf, feelies (movies), numerous varieties of scents, etc. However, the reverse process is also required – individuals and their desires have to conform to the physical environment. This process of controlling the conformity of the individual is enforced from the embryo. Individuals have predetermined roles in society – Alphas, Betas, Gammas, Deltas, Epsilons (Huxley 3,4). Some individuals are conditioned to be white collar citizens (Alphas), others are sewage workers (Epsilons) and in between are "standard Gammas, [and] unvarying Deltas" (Huxley 6).

According to Postman, Huxley's vision exemplifies an environment completely dominated by show business (80), where concealment of totalitarian tendencies is unnecessary in a society "narcotized by technological diversions" (111). While Orwellian societies are limiting access to knowledge, Huxlean societies are enlarging it (Postman 141). Either way, the population knows less. According to Postman, both authors show the withering of culture – Orwell through turning it into a prison, while Huxley turns it into a travesty (155). Today we are presented with both methods. The information flow is abundant from professional (news channels), non-professional (YouTube vloggers), or purely speculative sources (conspiracy theory sites). We are also bombarded with a myriad of entertainment outlets – shows on different platforms, movies, online games, interactive games and home games. Unfortunately, these entertainment outlets are

accumulating our viewing habits and providing us with additional choices based on our past viewing content[15].

Audio beacon technologies add another layer to entertainment surveillance. Installed in mobile phones, they capture TV viewing habits which provide additional content information. Social media sites connect and update us with our preferred content, while simultaneously studying user behavior and ways to influence it. Entertainment in its various forms masks and normalizes surveillance technology. Entertainment surveillance allows for unlimited online freedom, but the price is unlimited surveillance, a state which I call digital paradox and which I characterize further in Chapter 11.

15 Detailed reading of Orwell's *Nineteen Eighty-Four* and Huxley's *Brave New World* shows another technique implemented by both ruling parties – the decimation of the family unit. This policy helps isolate the individual as an entity and thus weakens it by eliminating the meaningful formation of confidential and trustworthy relationships in a family environment. In *Nineteen Eighty-Four* the destruction of the family is achieved by encouraging spying among family members and by the Party approving all marital unions. The family is completely eradicated in Huxley's *Brave New World* and one of the main slogans stated many times throughout the book confirms it – "every one belongs to every one else" (43). However, this aspect will not be explored further because it is beyond the scope of this thesis. Regardless, I hope that this insight encourages further research and opens doors for scholarly discussion.

CHAPTER 10 – MOTIVATION, MITIGATING ACTIONS AND CONCLUSION

This chapter will examine the motivation of the ruling Party in Orwell's *Nineteen Eighty-Four.* The motive presented by Orwell will be further connected to Foucault's exploration of the power-knowledge system. This chapter will tour actions that can mitigate surveillance methods in general and surveillance affordances in particularly by audio beacon technologies. The chapter will end with the conclusion and the findings yielded by this research. Those will be separated into two categories – findings regarding audio beacon technologies and findings related to George Orwell's *Nineteen Eighty-Four.*

10.1 – Motivation

Boyd and Crawford observe that technologies are not neutral or objective (662). Cathy O'Neil agrees that algorithms are subjective, created with specific goals in mind, often financial (qtd. in Orlowski 00:47:38-00:48:03). However, John Havens observes we could reach a state at which peoples' data is no longer needed and therefore the only valuable actions of an individual would be the one that leads to another purchase (65). According to him, the tracking and aggregation of all human actions will lead to exhausting variable information. This will render individuals' data useless and thus, human life experiences will not be regarded as valuable to the system unless an individual makes a purchase (Havens 65).

Dorfman points out that surveillance is far more dangerous than just eliminating privacy because surveillance is related to power and control (qtd. in Giroux "Totalitarian Paranoia" 130). Julie Cohen ties together surveillance and power by drawing examples from everyday language. In the Judeo-Christian religion, God is *all-seeing* and when individuals comprehend a situation, they are *seeing it* (Cohen 184,185). When referencing leaders or supervisors as overseers, seeing is a state of power (Cohen 184). Christopher Wylie, a former Cambridge Analytica data scientist turned activist, describes the technological paradigm as a battlefield (Wylie 00:05:38-00:09:59). Prior to working for Cambridge Analytica he worked for a military contractor serving NATO, the Pentagon and the Ministry of Defense. He says information is one of the five aspects of battle-space in the military. Based on his experience with military personnel, he states that domination is the primary objective of military strategy. The goal is to create information asymmetry. To triumph over your adversaries you have to gather as much information as

possible so you can manipulate them (Wylie 00:06:35-00:10:53). This is accomplished through algorithms (Wylie 00:09:25-00:09:59).[16]

In Orwell's *Nineteen Eighty-Four*, the Party's interest is knowing the thoughts of the populace in order to change their thinking (253). Individuals are a "flaw in the pattern" (Orwell, *Nineteen Eighty-Four* 255) to conformity. Once the Party "squeeze[s] you empty … then [it can] fill you with [themselves]" (Orwell, *Nineteen Eighty-Four* 256). Meaning, knowing the thoughts of individuals allows the ruling Party to use the most appropriate tactic to manipulate them. This in turn will yield the ability to change the person into conformity. The higher objective in Oceania is power – "We are not interested in the good of others; we are interested solely in power … only power, pure power" (Orwell, *Nineteen Eighty-Four* 263). People are left defenseless with this simple and crystal clear explanation. Power over the mind as an end objective begets the slogan "Freedom is slavery" (Orwell, *Nineteen Eighty-Four* 264). Once an individual succumbs, they are free to roam within the system. If human consciousness is the barometer of reality, then subjugation allows the Party to control it (Orwell, *Nineteen Eighty-Four* 265).

Audio beacon technologies, with their inherent feature of audio transmission, allow for the recording of thoughts and feelings. This data feed can be combined with predictive algorithms and thus reveal a comprehensive digital picture of individuals. This can be used for commercial reasons today, but the accumulation of data and the ability to be saved for secondary purposes allows the same data to be employed for opportunistic purposes in the future. Further, the data accumulation is not restricted to targeted individuals, but is an inherent feature of audio beacons, thus allowing mass surveillance of lawful individuals.

Foucault elucidates that the history of oppression in the 18th and early 19th centuries has a watershed moment when those in power realized that surveillance over the people is more efficient and profitable than public punishment (*Power* 38). To Foucault, new information creates new knowledge (*Power* 51) and this power-knowledge

16 The subject of war leads us back to Orwell's world of Oceania where the main goal is to maintain the state of war, constantly (*Nineteen Eighty-Four* 192). To draw the contemporary counterpart we will turn to Kate Epstein. She argues that the Patriot Act and its subsequent legislations not only increased government surveillance, but transformed the Cold War against "Communism" to the war against "Terrorism" (Epstein). The executive vice-chairman of the War Production Board during the Second World War, Charles Wilson, commented that a permanent war economy is what the United States needed (Stone 00:44:40-00:44:50).

system necessitates each other (*Power* 52). If we analyze audio beacons in terms of generating data, then the extraction of personal data can be studied as a form of a concealed power. According to Foucault, if surveillance and accompanying predictability algorithms cease to exist, the powerful would lose their power (*Power* 72).

Havens concurs that the life force of control through imbalance of power is sustained by complete ignorance of the people how their data is being used (191). If individuals were aware of the information being aggregated and its usage, the power would shift back to them. Their refusal to relinquish data or not would shift the power paradigm irreversibly (Havens 191). As we are not consulted beforehand, the obvious conclusion is that the data being collected is of no benefit to the people (Havens 195). According to Perinan, this relationship imbalance effectively eliminates solutions to privacy violations (187). Orwell names this paradigm of consumer ignorance "a single equation with two unknowns"(*Nineteen Eighty-Four* 74). If we know one side of the equation then we can make an intelligent decision about the opposite side.

Rudolph Rummel warns of this grave situation. In his book, *Death by Government,* Rummel writes the murders committed by authoritarian regimes can be compared with death counts during war. Killings committed by non-democratic governments are in major excess of human casualties during 20th century wars (Rummel 3). Non-democratic governments commit genocide against dissident groups and their own citizens, which Rummel labels "democide" (Rummel 1). The conclusion being non-democratic governments are more lethal than wars. Rummel finds power is a mandatory pre-requisite to commit democide (20) and absolute power breeds violence (1,2).

10.2 – Personal Devices

Velden distinguishes two ways that digital devices transmit information – insertion and leakage. Insertion is when the NSA implants malware in digital devices of people they want to monitor (Velden 186). Leakage is the assembly of prodigious personal data from phone calls, text messages, social media, search queries, website traffic and third party aggregated data (Velden 186). It is not random that the terms are sexually suggestive. All data is intimate and unique to the user.

Leaking data is not a secondary feature of audio beacon technologies, but rather their intended purpose. Audio beacons are instrumental in correlating behavior across different devices and they have the ability to de-anonymize individuals, resulting in loss

of privacy and freedoms as they nourish surveillance capitalism and expand the power imbalance. The data can be used against the data generator, so audio beacons are self-implicating technologies. They leak information by design, which reverses the definition of 'personal device.' Wendy Chun argues that digital devices are understood as personal due to “branding efforts” (qtd. in Velden 190). I agree with her and expand that mobile phones with apps implementing audio beacon technologies are personal but not because we own them, rather because they transmit personal data. Velden also states that digital devices “lead their own life” (189) and they do not belong to the user entirely.

10.3 – Mitigating the Surveillance Effect

There are three types of actions to mitigate the mass surveillance tracking by audio beacon technologies – individual actions, self-regulation and government legislation.

10.3.1 – Individual Actions

Privacy is both transactional and relational. It is transactional as it relies on a simple system of allowing access to personal data (or not). It is relational as in the act of sharing information, one can also inadvertently share the information of others. Collateral data sharing from audio beacons might involve a person’s tone of voice, psychological condition and the content of conversations.

The creation of audio beacon technologies may have originated from a commercial desire for market share and wealth, but the risk of their realization is detriment to the populace. The acute remedy is personal accountability. We have denial privileges for every app on our devices and can turn off microphone access. Many apps do not require the microphone to serve the needs of consumers. This one simple action will minimize the cog in the machine of data aggregation and will result in wider social impact.

10.3.2 – Self-Regulation

The second option of mitigating falls on corporations to self-regulate their actions of collecting data and to build products that are privacy oriented.

Rodrigues et al. explore the practice of distributing privacy seals by private companies certifying another company complies with a specific privacy criterion through

self-regulation. These seals are designed to ensure users of enhanced privacy practices of said organization (Rodrigues et al. 101). Researchers conclude that companies issuing privacy seals have a conflict of interest as they are dependent on the funds received from these certified companies (Rodrigues et al. 108). This contradiction leads to an opposing outcome. LaRose and Rifon report that companies displaying TRUSTe and BBBOnLine privacy seals are more inclined to violate users' privacy by collecting unnecessary data (qtd. in Rodrigues et al. 106). Therefore, the race for increasing revenue handicaps privacy initiatives that appear to be in users' favor. When it comes to privacy legislation, Lessig notes, in support of Zittrain's view that legislation follows the money (qtd. in Lessig 251), that although we have financial privacy laws, individual privacy is left to the free market. Perinan agrees that conflict of interest prohibits finding solutions to the privacy problem (187). These statements lead us to the third and more robust solution of mitigating audio beacon surveillance – government legislation.

10.3.3 – Government Legislation

In the course of daily operations, governments are empowered to enforce the rule of law, yet the law has to guarantee the protection of the citizens against the government (Dumortier and Goemans 5). It is a conundrum – we protect our privacy from the government and simultaneously require the government to quash intrusions of our privacy from others (Hirshleifer 651). The unfortunate contradiction occurs, as Schneier observes, as the government buys or extracts data from corporations and in turn ensures that companies can collect as much data as possible (Schneier).

Based on information released by whistleblowers Edward Snowden and Chelsea Manning, governmental agencies in the USA are indiscriminately gathering all possible data. A mode of aggregation Velden calls "collect it all" (182). As discussed previously, the third party doctrine allows government and private organizations to acquire any and all data to their satisfaction. In addition to purchasing data, governmental agencies can install backdoors into a company's software allowing them full access (Velden 187). Velden examines the NSA and their modification to Google cookies which converted them into a surveillance instrument (190). The NSA is only one of seventeen agencies within the US Intelligence Community. Their combined budget for 2010 was $80 billion dollars, twelve times the budget from 1998 (Dilanian).

According to Giroux, the creation of fusion centers, where data from private corporations is merged with governmental data, local data and international data, is a prime example of the marriage between corporate and government surveillance ("Totalitarian Paranoia" 118). Fuchs sites another example of the Prism and Tempura surveillance systems and their partnership between the government and private companies (7), that produces "totalitarian surveillance systems … that centralizes control by monitoring decentralized technologies" (8).

10.4 – Data as God

"The world is reborn as data and the electronic text is universal in scale and scope" (Zuboff, "Big Other" 77). This quote from Zuboff alludes to a biblical passage. Havens equates "scientific determinism … to religious faith" (104) and Kate Crawford and Jason Schultz recognize that one aspect of Big Data is the belief that it provides greater accuracy and truth ("Big Data" 96). Niranjan Rajah proposes a consilience of traditional and contemporary cultures of prediction and decision making. He suggests that the increasing reliance on predictive capacities based on big data analytics brings contemporary society in alignment with the astrological determinism of the past (Rajah). According to Boyd and Crawford, Big Data is not necessarily big, or new. They trace the accumulation of data into databases back to the late 19th century and denote that the term *big* refers to the ability of different data sets to be cross-referenced (Boyd and Crawford 663,664).

Further, as all data is interpreted, objectivity claims are problematic (Boyd and Crawford 666), especially when the questions asked depend on who the researchers are (Boyd and Crawford 674). Thus, the same data set can yield different meanings and, more importantly, is impossible to reproduce (Boyd and Crawford 673,674). The reliability of the interpretations of studies based on Big Data, does not hinder its actual accumulation by big tech companies. As seen in Chapters 8 and 9, the aggregation of Big Data is based as much on its behavior altering capabilities as on its use in the prediction of behavior.

10.5 – Conclusion

John Frank Weaver argues the need for new privacy laws by stating that present laws protecting individual privacy were developed without considering the

implementation of AI surveillance technologies (qtd. in Havens 89). According to former product manager of NVIDIA, Randima Fernando, the processing power of computers has increased a trillion times from the 1960s to today. Correspondingly, the span yielded no development of human intellect (Orlowski 00:44:58-00:45:32). Winkler and Rinner agree that the development of surveillance technologies are increasing exponentially faster than governmental regulations (103). Karyda et al. respond that believing digital environments are benefiting us, improving our lives, providing more cost efficiency, convenience and safety is merely an assumption (195). Digitizing of entertainment can act as a veil, obscuring the surveillance paradigm that is unprecedented in the history of our existence.

The findings are split into two sections. The first one relates to findings about audio beacon technologies, while the ancillary findings are related to George Orwell's *Nineteen Eighty-Four*.

The broad conclusion found through this research is that audio beacon technologies are enhancing the surveillance paradigm. There are five specific findings:
1) Continuous capture of the surrounding environment while actively broadcasting their pin-point position, ultrasound beacons are a typical surveillance technology.
2) They can transmit our thoughts and feelings in the most intimate of spaces, violating Nissenbaum's theory of privacy as contextual integrity by breaking the norms of appropriateness and flow (qtd. in Lutz and Newlands 148).
3) The implementation of audio beacon technologies allows surveillance on a mass scale. This mode of covert listening eliminates the targeted surveillance practices of previous generations and enables surveillance of law-abiding citizens.
4) As such, audio beacon technologies are enhancing the rising web of surveillance and are contributing to the unbalanced power paradigm.
5) The general conclusion formed is that these technologies can serve as a surveillance method, enhancing authoritarian and exploitative regimes.

Every family conversation, happy moment or embarrassing disagreement can no longer be shielded by simply closing doors, window blinds or whispering. The data is aggregated for posterity and can be used against us by private or public organizations. Corporations can use it for seemingly mundane reasons, such as swaying us to buy Coca Cola instead of Mountain Dew. Or for nefarious purposes – raising insurance rates, social order implementation and social credit generation, to name a few.

Governments can use it to dissuade dissent, to track and profile groups and organizations and largely to advance an agenda without our conscious awareness of being manipulated.

Looking at audio beacon technologies, I have found two insights about Orwell's *Nineteen Eighty-Four.* The insights include the five methods of surveillance aided by three additional factors and the fact that Orwell's symbol of surveillance and oppression, the boot, has morphed into Huxley's method of control, soma.

The methods of surveillance are – ground patrols, helicopters, encouraging self-spying among citizens, video surveillance and microphones. The three factors helping the complete control of the Party and the manipulation techniques are – language use, propaganda and altering the past. Another finding is that the proles' neighborhood is a place where members of the Thought Police reside. The proles are viewed as a population exempt from surveillance practices through the eyes of Winston. Julia also roams the streets of the same neighborhood, so we can assume that she believes the same. However, they are wrong. The neighborhood where the proles live is falsely labeled by the Party as a surveillance-free environment from the Party in an attempt to capture dissidents. As observed earlier Mr. Charrington, a member of the Thought Police, lives and has a business there. This deceptive behavior leads to the capture of Winston and Julia.

The second finding is that Orwell's *Nineteen Eighty-Four* is not sufficient enough to portray contemporary society, because entertainment is missing from the world of Oceania. To paint a comprehensive picture of today's digital environment, the assistance of Huxley's *Brave New World* is necessary. Using both dystopian fictions as complimentary, not contradictory sources, I have found that surveillance practices today are disguised as entertainment. As such, the boot, Orwell's symbol of surveillance and oppression, has turned into Huxley's symbol of control, the chemical compound, soma. The relationship between these two elements will be further explored next in Chapter 11.

10.5.1 – Solutions

This state leaves individuals with two meaningful measures – individual action and lobbying local government officials. The former will have an immediate consequence on individuals' data transmission. The latter offers a more robust solution, yet possibly taking longer to carry out. The immediate action of refusing microphone permission in all

apps that do not require it would mitigate audio data collection. Concerning location data, individuals can refuse location permission to apps not in need. To mitigate the use of Google cookies, individuals can use search engines that do not collect personal data, such as Qwant or DuckDuckGo. In communication apps that require audio, video and text data users can choose Signal – Private Messenger. To avoid Google's collection of email data, users can switch to ProtonMail.

The overall purpose of this research is to raise public awareness of audio beacons, their surveillance capabilities and the connected privacy implications. Simultaneously, this research is hoping to encourage individuals to contact their local representatives and lobby for better privacy laws protecting consumers. This tactic may be more time consuming, but it is the clearcut solution to rampant surveillance practices using audio beacon technologies. Privacy legislation will ensure the long-term protection of individuals. The government as a social institution is tasked with the wellbeing of its citizens, therefore privacy legislation will mitigate opportunistic corporate practices engaged only for mercantile reasons.

CHAPTER 11 – THE DIGITAL PARADOX

11.1 – Both Sides of the Same Coin

The beginning of the 21st century presents us with a paradox. On the one hand, we are free to roam online, read various interpretations on any subject, express our opinions and exchange ideas liberally with anyone we choose. On the other side, our actions are surveilled, our data is aggregated and we are subject to behavior manipulation. Many of the privacy and surveillance challenges faced today did not occur as a result of coercion, but in the course of voluntary activities that are carelessly enjoyed as entertainment. Contemporary digital society incorporates mass surveillance and new forms of entertainment intertwined in a paradoxical relationship. Huxley's *Brave New World* does not address mass surveillance and conversely, Orwell's *Nineteen Eighty-Four* omits entertainment. Given these blind spots in these two projected futures, I suggest that the contemporary social order is best analyzed and reflected upon using a combination of Orwell's and Huxley's visions.

Regarding both visions of authoritarian regimes as complimentary is not a new one. According to Henry Giroux, both books work together to examine current authoritarian tendencies in the USA ("Orwell, Huxley"). He addresses unwarranted governmental surveillance in the USA, militarization of police, dispersement of peaceful protests, racial profiling and suppression of dissent, labeling it terrorism (Giroux, "Orwell, Huxley").

In the context of this research on audio beacons, a significant similarity between Huxley's and Orwell's worlds is that microphones play a significant role within the surveillance apparatus of the state. In *Nineteen Eighty-Four,* they are used to capture the inner feelings of Winston and Julia. In *Brave New World*, microphones are used to spy on John (the Savage) and to capture his internal state. This leads to elimination of his privacy and ultimately to his death (Huxley 260).

The books overlap in their connection to the act of reading. In *Nineteen Eighty-Four*, Winston is tasked with rewriting the content of written media. Books are rewritten and altered to match current Party doctrine and those that remain original are banned or destroyed, as it was with Emmanuel Goldstein (Orwell, *Nineteen Eighty-Four* 39,40). A similar situation exists in Huxley's *Brave New World*, where books are banned (51)

because they will obstruct the conformity of the populace (226) and individuals are conditioned to hate books altogether (21).

Another connection between the books is the use of slogans. Orwell uses several slogans for propaganda purposes – “War is Peace, Freedom is Slavery, Ignorance is Strength” (*Nineteen Eighty-Four* 4). *Brave New World* uses slogans to condition the populace – “Ending is better than mending” (Huxley 49), “Gramme is better than damn” (Huxley 54), “When the individual feels, the community reels” (Huxley 94). The most popular contemporary slogan respective to privacy is “If you’ve got nothing to hide, you’ve got nothing to fear” (Solove 2,3). Also called the “nothing to hide” argument, this slogan is a continuation of the privacy-security dichotomy (Solove 7) explored in Chapter 9. According to Solove, the slogan undermines the value of privacy by positing it as a question that affects isolated individuals (23). This eliminates the social impact of mass surveillance (Solove 23) and shifts the power balance toward institutions and governments (Solove 10).

Eradicating history is another practice that is promoted by the totalitarian leaders of Oceania and London. In Orwell’s world, historical facts are constantly updated to match the present. In Huxley’s world, the Controller proclaims “History is bunk” (34). In both societies, altering historical documents has an anti-democratic effect. The contemporary counterpart of these practices was observed in Chapter 9 with Google's changing of their original privacy policy. The initial privacy policy was written with consideration for user privacy, which is in direct opposition to Google’s current mass surveillance business program (Hoback 00:12:00-00:13:00).

11.2 – Epilogue: The Digital Paradox Society

The fictional worlds of Orwell and Huxley present opposite environments, but are equally concerned with power. Both societies are completely dominated by the ruling party, but their execution takes different routes. If we marry these two visions of totalitarian society, we recognize the two faces of contemporary society. On one side, we have a power imbalance enhanced by digital algorithms which is reminiscent of Orwell’s vision. On the other side, we have entertainment surveillance, reminiscent of Huxley’s vision. Entertainment offers distraction for individuals and shifts the point-of-view away from surveillance practices. Entertainment surveillance nourishes a state where an “army of managers control[s] a population of slaves who do not have to be

coerced, because they love their servitude" (Huxley XV). Without entertainment surveillance, the system will collapse and it will resemble Orwell's world with its gaudy display of power.

In the digital paradox today two types of protections, constitutional law and regulatory law, have "learned how to use the other's laws to bypass their own restrictions" (Schneier). The result is the denial of privacy protection through a hidden process which masks personal harm. Citizens can be covertly penalized within an imposed social order of totalitarian measures.

Contemporary society has its roots in the previous discipline society as seen from Foucault's description of the utopian legal penalty system – "deprive the prisoner of all rights, but do not inflict pain; impose penalties free of all pain" (*Discipline* 11). The system focuses on gathering information not about the past, but rather on current activities that provide additional insights revealing their potential of committing future crimes (Foucault, *Discipline* 126). In this penal system, punishment is carried out to transform the criminal (Foucault, *Discipline* 127), while in the digital paradox, behavior modification is targeted towards mercantile goals. As examined in prior sections, audio beacon technologies are linking multiple devices, making it possible to de-anonymize an individual. This action imposes geographic constraints on the individual due to accurately located data within a confined space. Moreover, people are unaware of the continuous data capture and cross-device identification.

For Foucault, an integral part of the process emerges from meticulous records of individuals' habits (*Discipline* 129). The emergence of fusion centers, where different types of data are linked to reveal the full digital identity of a person, takes this idea one step further. According to Foucault, this process obscures its own manifestation prohibiting the individual's involvement (*Discipline* 129). In the digital paradox society, this is ensured by the proprietary nature of data and the absence of disclosure of how algorithms work, what information they gather and how this information is used. The elimination of interference from outside forces succeeds by the scarcity of government legislation.

To ensure the order's disciplinary power over the individual, Foucault observes that the visibility of the populace is paramount – "their visibility assures the hold of the power that is exercised over them" (*Discipline* 187). However, in the digital paradox society, the presence of power does not need to be overtly demonstrated. The exercise

of power is masked by on-demand entertainment, games and instant gratification commercialism. In this way, I argue that today's society is a combination of both dystopian and utopian tendencies mixed in a digital paradox. On one hand, we are subjected to penetrating tracking practices that make Orwell's vision of surveillance in Oceania seem infantile (Haggerty and Ericson 612). On the other hand, we are inundated by technologies that make our lives convenient and allay boredom. Digital technologies allow us to travel virtually to any part of the globe, connect with loved ones instantly, discover long lost family members, and even locate organ donors. This thesis began with a quote from Orwell's *Nineteen Eighty-Four* - "If you want a picture of the future, imagine a boot stamping on a human face – forever" (267). For Orwell, the "boot stamping on a human face" (*Nineteen Eighty-Four* 267) is a symbol for the completely surveilled and oppressed society. In the digital paradox society, with its entertainment surveillance, Huxley's soma has become Orwell's boot.

In fact, the discernible aspects of the contemporary digital environment astonishes us with its variety, usability and lightheartedness. Reminiscent of characters in Huxley's *Brave New World,* we need our daily ration of the custom-designed advertisement popping up at the right moment to fill the gap between loneliness and desire. This accords with Foucault's idea of how discipline over the body can function – it increases utility and concurrently decreases political disobedience (*Discipline* 138). In the digital paradox societies such as ours, extraordinary measures to protect individual privacy are not only desirable, they are imperative.

REFERENCES

Aguilera, Teodoro et al. “Broadband Acoustic Local Positioning System for Mobile Devices with Multiple Access Interference Cancellation.” *Measurement,* vol.116*,* 2018, pp.483-494*.*

Arp, Daniel et al. “Privacy Threats Through Ultrasonic Side Channels on Mobile Devices.” 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 2017-04, pp.35-47.

Ashbrook, Daniel., Starner, Thad. “Using GPS to Learn Significant Locations and Predict Movement Across Multiple Users.” *Personal and Ubiquitous Computing*, vol.7, 2003, pp.275-286.

Atrey, Pradeep K. et al. “Audio Based Event Detection for Multimedia Surveillance.” *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, *IEEE, 5, 2006,* pp.813–816.

Ball, Philip. “In Retrospect: Brave New World.” *Nature*, vol.503, 2013, pp.338-339.

Bennett, Colin, J. *The Privacy Advocates: Resisting the Spread of Surveillance*. Massachusetts Institute of Technology, 2008.

Bolin, Paul E. “For the Future, For the Unborn”: Considerations of History and Historians for Art Educators, Generated From George Orwell’s Novel 1984.” *Studies in Art Education: A Journal of Issues and Research*, vol.58, no.2, 2017, pp.88-99.

Boyd, Danah., Crawford, Kate.“Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon.” *Information, Communication & Society,* vol.15, 2012, pp.662-679.

Burgin, Paul. “Never Alone: Why the Inevitable Influx of Drones Necessitates a New Fourth Amendment Standard that Adequately Protects Reasonable Expectations of Privacy.” *University of Baltimore Law Review*, vol. 45, no.3, article 5, pp.514-560, 2016.

Butler, Christopher. “Visa makes strategic investment in LISNR, a start-up that wants to rival technology used by Apple Pay.” *CNBC Disruptor 50*, 5 November 2019, https://www.cnbc.com/2019/11/05/visa-invests-in-lisnr-a-start-up-that-wants-to-rival-apple-pay.html. Accessed 21 May 2021.

Callon, Michel. “Four Models for the Dynamics of Science.” *Handbook of Science and Technology Studies*, edited by Sheila Jasanoff, Gerald E. Markle, James C. Peterson & Trevor Pinch, SAGE Publications Inc., 2011, pp.28-63.

Carr, Nicholas G. “Hypermediation: Commerce as Clickstream.” *Harvard Business Review*, vol.78, no.1, 2000, pp.46-48.

Cohen, Julie, E. “Privacy, Visibility, Transparency, and Exposure.” *The University of Chicago Law Review*, vol.75, no.1, 2008, pp.181-201.

Constandache, Ionut et al. “Daredevil: Indoor Location Using Sound.” *Mobile Computing and Communications Review*, vol.18, no.2, 2014, pp.9-19.

Crawford, Kate., Joier, Vladan. “Anatomy of AI System.” Anatomyof. https.//anatomyof.ai/. 2018, Accessed on April 3, 2021.

Crawford, Kate., Schultz, Jason. “Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms.” *Boston College Law Review*, vol.55, no.1, 2014, pp.93-128.

Crocco, Marco et al. “Audio Surveillance: A Systematic Review.” *ACM Computing Surveys,* vol.48, no.4, article 52, 2016, pp.1-46.

CSP. “ExxonMobil Partners with Shopkick.” *CSP Daily News,* 3 April 2012, https://www.cspdailynews.com/technologyservices/exxonmobil-partners-shopkick. Accessed 21 May 2021.

Deleuze, Gilles. “Postscript on the Societies of Control.” *October,* vol.59 (Winter, 1992), pp.3-7.

Desai, Anuj, C. “Wiretapping Before the Wires: The Post Office and the Birth of Communication Privacy.” *Stanford Law Review*, vol.60, no.2, 2007, pp.553-594.

Dickstein, Morris. “Hope Against Hope: Orwell’s Posthumous Novel.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.63-73.

Dilanian, Ken. “Overall U.S. Intelligence budget tops $80 billion.” *Los Angeles Times*, 28 October 2010, https://www.latimes.com/archives/la-xpm-2010-oct-28-la-na-intel-budget-20101029-story.html. Accessed 24 May 2021.

Dumortier, Jos., Goemans, Caroline. “Roadmap for European Legal Research in Privacy and Identify Management.” European Commission, DG Information Society, IST Programme, RAPID Project, 2003, pp.1-27.

Edge, David. “Reinventing the Wheel.” *Handbook of Science and Technology Studies*, edited by Sheila Jasanoff, Gerald E. Markle, James C. Peterson & Trevor Pinch, SAGE Publications Inc., 2011, pp.2-23.

Epstein, Kate. “Total Surveillance.” *CounterPunch*, 28 June 2013, https://www.counterpunch.org/2013/06/28/total-surveillance/print/. Accessed 24 May 2021.

Filonenko, Viacheslav et al. “Investigating Ultrasonic Positioning on Mobile Phones.” 2010 International Conference on Indoor Positioning and Indoor Navigation (IPIN), 15-17 September 2010, Zurich, Switzerland.

Flynn, Kerry. “With Beacons and Audio, LISNR uses proximity Marketing to Amplify Listeners.” *Forbes*, 30 July 2014, https://www.forbes.com/sites/kerryflynn2014/07/30/with-beacons-and-audio-lisnr-uses-proximity-marketing-to-amplify-listeners/.Accessed 21 May 2021.

Forbes. “Shopkick,” *Forbes*, https://www.forbes.com/companies/shopkick/. Accessed 21 May 2021.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison.* Translated by Alan Sheridan, Second Edition, New York, Vintage Books A Division of Random House Inc., 1995.

Foucault, Michel. *Power/Knowledge: Selected Interviews and Other Writings 1972-1977,* Edited by Colin Gordon, Translated by Colin Gordon, Leo Marshall, John Mepham, Kate Soper, New York, NY Pantheon Books, Harvester Press 1980.

Friedewald, Michael et al. “Seven Types of Privacy.” *Springer Science+Business Media Dordrecht*, January 2013, pp.1-26.

Fuchs, Christian. “Surveillance and Critical Theory.” *Media and Communication*, vol. 2, no. 2, 2015, pp.6-9.

Galic, Masa et al. “Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation.” *Philos.Technol.,* vol.30, 2017, pp.9-37.

Gillum, Jack et al. “FBI Behind Mysterious Surveillance Aircraft over US Cities.” Associated Press. https://apnews.com/article/4b3f220e33b64123a3909c60845da045. June 2, 2015, Accessed on March 30, 2021.

Giroux, Henry, A. “Totalitarian Paranoia in the Post-Orwellian Surveillance State.” *Cultural Studies,* vol.29, no.2, 2015, pp.108-140.

Giroux, Henry, A. “Orwell, Huxley and the Scourge of the Surveillance State.” *Thruthout*, 30 June 2015, https://truthout.org/articles/orwell-huxley-and-the-scourge-of-the-surveillance-state/. Accessed 20 May, 2021.

Gitlin, Todd. “Varieties of Patriotic Experience.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.126-144.

Goldfarb, Avi. Tucker, Catherine. E. “Privacy Regulation and Online Advertising.” *Management Science,* vol.57, no.1, January 2011, pp.57-71.

Google. “Google Privacy Policy,” *Google*, https://www.gstatic.com/policies/privacy/pdf/pdf/20210204/3jla0xz1/google_privacy_policy_en_eu.pdf. Accessed 21 May 2021.

Gottlieb, Erika. “Orwell’s Satirical Vision on the Screen: The Film Versions of Animal Farm and Nineteen Eighty-Four.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.252-263.

Haggerty, Kevin D., Ericson, Richard V. “The Surveillant Assemblage.” *British Journal of Sociology,* vol.51, no.4, 2000, pp.605-622.

Hamamra, Bilal Tawfig. “A Foucauldian Reading of Huxley’s Brave New World.” *Theory and Practice in Language Studies*, vol.7, no.1, January 2017, pp.12-17.

Haraway, Donna. “A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century.” *Simians, Cyborgs and Women: The Reinvention of Nature,* New York, NY, Routledge, 1991, pp.149-181.

Harma, Aki et al. “Automatic Surveillance of the Acoustic Activity in our Living Environment.” *Proceedings of the IEEE International Conference on Multimedia and Expo, IEEE*, 4, 2005.

Hartzog, Woodrow. “The Fight to Frame Privacy.” *Michigan Law Review*, vol.111, no.6, April 2013, pp.1021-1043.

Harvey, David. “Education, Part 1, Reading Marx’s “Capital” Volume 1 with David Harvey.” *YouTube*, uploaded by The People’s Forum NYC, 7 March 2019, https://www.youtube.com/watch?v=n5vu4MpYgUo, Accessed 31 July, 2021.

Harvey, David. “Education, Part 3, Reading Marx’s “Capital” Volume 1 with David Harvey.” *YouTube*, uploaded by The People’s Forum NYC, 7 March 2019, https://www.youtube.com/watch?v=cpW1Q9sgUB0, Accessed 31 July, 2021.

Havens, John C. *Heartifical Intelligence*. New York, NY. 10014, USA, Jeremy P. Tarcher/Penguin, 2016.

Heerden, Alastair et al. “In-Home Passive Sensor Data Collection and Its Implications for Social Media Research: Perspectives of Community Women in Rural South Africa.” *Journal of Empirical Research on Human Research Ethics*, vol.1, no.11, 2019, pp.1-11.

Hirshleifer, Jack. “Privacy: Its Origins, Function, and Nature.” *The Journal of Legal Studies*, vol.9, no.4, 1980, pp.649-664.

Hoback, Cullen, director. *Terms and Conditions may Apply*. Hyrax Films, Topiary Productions, 2013.

Hollander, John. “The Language of Privacy.” *Social Research,* vol.68, no.1, 2001, pp.5-28.

Hon, Tsz-Kin et al. “Audio Fingerprinting for Multi-Device Self-Localization.” *IEEE/ACM Transactions on Audio, Speech, and Language*, vol.23, no.10, 2015, pp.1623-1636.

Hong, Sun-Ha. “Privacy Must be Defended.” *The New Rambler*, https://newramblerreview.com/book-reviews/law/privacy-must-be-defended. Accessed 24 April, 2021.

Hunter, Lynette. “Prescience and Resilience in George Orwell’s Political Aesthetics.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.229-242.

Huxley, Aldous. *Brave New World*. New York, NY, 10022, USA, Harper & Row, 1969.

Igo, Sarah, E. *The Known Citizen: A History of Privacy in Modern America*. Cambridge, Massachusetts, USA, Harvard University Press, 2018.

Imber, Jonathan B. “Orwell in an Age of Celebrity.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.178-184.

Ka, Soonwon et al. “Near-Ultrasound Communication for TV’s 2nd Screen Services.” MobiCom ‘16, 3-7 October 2016, New York City, NY, USA, 2016, pp.42-54.

Karyda, Maria et al. “Privacy and Fair Information Practices in Ubiquitous Environments.” *Internet Research,* vol.19, no.2, 2015, pp.194-206.

Kaspersky. “What are Cookies?” *Kaspersky.* https://www.kaspersky.com/resource-center/definitions/cookies. Accessed 30 June 2021.

Knappenberger, Brian, director. *Truth and Power: The Stingray – Season 1, Episode 3*, Luminant Media, 2016.

Lauer, Josh. “Surveillance History and the History of New Media: An Evidential Paradigm.” *New Media & Society*, 2011, vol. 14, no.4, pp.566-592.

Lessig, Lawrence. “Privacy as Property.” *Social Research,* vol.69, no.1, Spring 2002, pp.247-269.

Lisnr. “Privacy Policy,” *Lisnr*, https://lisnr.com/privacy-policy/. Accessed 21 May, 2021.

Lisnr. “Trust Comes First at LISNR.” *Lisnr*, https://lisnr.com/partners/. Accessed 21 May 2021.

Lopes, Sergio I. Et al. “Accurate Smartphone Indoor Positioning Using a WSN Infrastructure and Non-invasive Audio for TDoA Estimation.” *Pervasive and Mobile Computing,* vol. 20, 2015, pp.29-46.

Lutz, Christoph., Newlands, Gemma. “Privacy and Smart Speakers: A Multi-Dimensional Approach.” *The Information Society*, vol.37, no.3, 2021, pp.147-162.

Lynn, Samara. “The Internet of Sound.” *Blackenterprise.com,* Samara Lynn ed., March 2016, Earl G. Graves Publishing Co., pp.29-31.

Maasen, Sabine et al., editors. *TechnoScienceSociety*. Cham, Switzerland, Springer Nature Switzerland AG, 2020.

Mavroudis, Vasilios et al. “On the Privacy and Security of the Ultrasound Ecosystem.” *Proceedings on Privacy Enhancing Technologies*, 2017, vol.2, pp.95-112.

Morozov, Evgeny. “Capitalism’s New Clothes.” *The Baffler*, 4 February 2019, https://thebaffler.com/latest/capitalisms-new-clothes-morozov. Accessed 8 May 2021.

Noyb. “Austrian DPA has Option to Fine Google up to €6 Billion,” *noyb*, 06 May 2021, https://noyb.eu/en/austrian-dpa-has-option-fine-google-eu6-billion. Accessed 31 July 2021.

Noyb. “Breaking: Austrian OGN Asks CJEU if Facebook “undermines” GDPR since 2018,” *noyb*, 20 July 2021, https://noyb.eu/en/breaking-austrian-ogh-asks-cjeu-if-facebook-undermines-gdpr-2018. Accessed 31 July 2021.

Noyb. “Data Transfers to the US and Insufficient Cookie Information: Noyb Filed Complaint on Behalf of six MEPs Against the European Parliament,” *noyb*, 22 January 2021, https://noyb.eu/en/data-transfers-us-and-insufficient-cookie-information-noyb-files-complaint-against-european, Accessed 31 July 2021.

Noyb. “Luxemburg’s watchdog Refuses to Show its Teeth to US Companies,” *noyb*, 25 January 2021, https://noyb.eu/en/luxemburgs-watchdog-refuses-show-its-teeth-us-companies, Accessed 31 July 2021.

Noyb. “Update on Noyb’s 101 Complaints on EU-US Data Transfers-Only One Country Shines,” *noyb*, 22 September 2020, https://noyb.eu/en/update-noybs-101-complaints-eu-us-data-transfers, Accessed 31 July 2021.

Orlowski, Jeff, director. *The Social Dilemma*, Exposure Labs, Argent Pictures, 2020.

Orwell, George. *Nineteen Eighty-Four*. New York, New York, 10014, USA, Signet Classics, 1950.

Orwell, George. “Politics and the English Language.” *The Norton Anthology of English Literature: Seventh Edition, Volume 2C, The Twentieth Century*, edited by Jon Stallworthy, M.H.Abrams, Stephen Greenblatt, W.W.Norton & Company, Inc, 2000, pp.2462-2471.

Pavlounis, Dimitrios. “Sound Evidence: An Archeology of Audio Recordings and Surveillance in Popular Film and Media.” *Core*, The Open University, 2016, https://core.ac.uk/display/73949421, Accessed 4 August 2021.

Peng, Chunyi et al. “BeepBeep: A High Accuracy Acoustic Ranging System using COTS Mobile Devices.” SenSys’07, 6-9 November 2007, Sydney, Australia.

Perinan, Bernardo. “The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law.” *American Journal of Legal History,* vol. 52, 2012, pp.183-201.

Petersen, Julie. *Introduction to Surveillance Studies*. Boca Raton, FL, 33487-2742, USA, Taylor & Francis Group LLC, 2013.

Pham, Quoc-Cuong et al. “Audio-video Surveillance System for Public Transportation.” *Proceedings of the 2nd International Conference on Image Processing Theory Tools and Applications, IEEE,* 2010, pp.47–53.

Posner, Richard, A.“The Economics of Privacy.” *The American Economic Review,* vol.71, no.2, 1981, pp.405-409.

Postman, Neil. *Amusing Ourselves to Death: Public Discourse in the age of Snow Business*. New York, New York, 10010, USA, Elisabeth Sifton books-Viking, 1985.

Radhakrishnan, Regunathan et al. “Systematic Acquisition of Audio Classes for Elevator Surveillance.” *Proceedings of SPIE,* 2005, pp.64-71.

Radin, Joanna. “The Speculative Present: How Michael Crichton Colonized the Future of Science and Technology.” *Osiris 2019*, vol.34, 2019, pp.297-315.

Rajah, Niranjan. “Towards a Post-Traditional Gnoseology of Potentiality and Prediction: Preliminaries.” Sublime Horizons. https://www.sublimehorizons.ca/towards-a-post-traditional-gnoseology-of-potentiality-and-prediction-preliminaries/#_ftnref40. Accessed 3 June 2021.

Reddy, Shankar, M.S. et al. “Probabilistic Detection Methods for Acoustic Surveillance Using Audio Histograms.” *Springer Science+Business Media*, vol.34, 2014, pp.1977-1992.

Rehbock, Billy. “Jaguar Land Rover Partners with Lisnr to Control Cars with Sound.” *Automobile*, 30 May 2017, https://www.automobilemag.com/news/jaguar-land-rover-partners-lisnr-control-cars-sound/. Accessed 21 May 2021.

Reidenberg, Joel R. et al. “Disagreeable Privacy Policies: Mismatches Between Meaning and Users’ Understanding.” Berkeley Technology Law Journal, vol.30, no.1, Spring 2015, pp.39-88.

Resnick, Stephen, A. “Econ 305, Lecture 1, Intro.” *YouTube*, uploaded by UmassEconomics, 16 May 2011, https://www.youtube.com/playlist?list=PL8B2364D7C0D31D63, Accessed 8 March 2021.

Rodden, John. “On the Ethics of Admiration – and Detraction.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.86-95.

Rodrigues, Rowena et al. “Developing a Privacy Seal Scheme (that works).” *International Data Privacy Law,* vol.3, no.2, 2013, pp.100-116.

Rose, Jonathan. “Abolishing the Orgasm: Orwell and the Politics of Sexual Persecution.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.23-44.

Rosenwald, Lawrence. “Orwell, Pacifism, Pacifists.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.111-125.

Rouas, Jean-Luc et al. “Audio Events Detection in Public Transport Vehicle.” *Proceedings of the 2006 IEEE Intelligent Transportation Systems Conference, IEEE*, 2006, pp.733–738.

Rubinstein, Ira S., Good, Nathaniel. “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents.” *Berkeley Technology Law Journal,* vol.28, no.2, 2013, pp.1333-1413.

Rummel, Rudolph, J. *Death by Government*. New York, New York. 10017, Routledge, 2017.

Schneier, Bruce. “The Public-Private Surveillance Partnership.” *Bloomberg*, 31 July 2013, https://www.bloomberg.com/opinion/articles/2013-07-31/the-public-private-surveillance-partnership. Accessed 12 June 2021.

Scolari, Carlos A. “From (New)Media to (Hyper)Mediations. Recovering Jesus Martín-Barbero’s Mediation Theory in the Age of Digital Communication and Cultural Convergence.” *Information, Communication & Society vol.*18, no.9, 2015, pp. 1092-1107.

Shanahan, Murray. *The Technological Singularity.* Cambridge, Massachusetts, The MIT Press, 2015.

Shopkick. “Become a Partner.” *Shopkick*, https://www.shopkick.com/. Accessed 21 May 2021.

Shopkick. “Shopkick Privacy Policy,” *Shopkick*, https://www.shopkick.com/privacy-policy. Accessed 21 May, 2021.

Signal. “Signal Terms & Privacy Policy,” *Signal*, https://signal.org/legal/. Accessed 21 May, 2021.

Silverpush. “Privacy Policy,” *Silverpush*, https://www.silverpush.co/privacy-policy/. Accessed 21 May, 2021.

Silverpush, “Silverpush Partners with Digital Commons to Provide its AI ad solutions in New Zealand.” Silverpush, 10 March 2020, https://www.silverpush.co/silverpush-partners-with-digital-commons/. Accessed 21 May 2021.

Sismondo, Sergio. *An Introduction to Science and Technology Studies.* Second edition, West Sussex, UK, Blackwell Publishing, 2010.

Skinner, Quentin. "Liberty, Liberalism and Surveillance: a Historic Overview." *openDemocracy*. https://www.opendemocracy.net/en/opendemocracyuk/liberty-liberalism-and-surveillance-historic-overview/. Accessed 11 May, 2021.

Slade, Hollie. "The $30M App that Rewards you for just Browsing." *Forbes*, 2 July 2014, https://www.forbes.com/sites/hollieslade/2014/07/02/the-30m-app-that-rewards-you-for-just-browsing/. Accessed 21 May 2021.

Slater, Ian. Orwell: *The Road to Airstrip One*. Second Edition, Montreal & Kingston, London, Ithaca, McGill-Queen's University Press, 2003.

Sleeper, Jim. "Orwell's 'Smell Little Orthodoxies.'" *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.160-177.

Smith, Adam. "Classical theory > Adam Smith > 1.1.16 Perfect Market." *Economics-reloaded*, http://economics-reloaded.com/1_classical_theory/Adam_Smith/1_1_16_perfect_market.htm. Accessed 10 May 2021.

Solove, Daniel J."I've got Nothing to Hide" and Other Misunderstandings of Privacy." *San Diego Law Review,* vol.44*,* 2007, pp.745-773.

Stark, Luke. "The Emotional Context of Information Privacy." *The Information Society,* vol.32, no.1, 2016, pp.14-27.

Statista. "Number of Monthly Active Facebook Users Worldwide as of 4th quarter 2020 (in millions)." *Statista.com*. www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. Accessed April 1, 2021.

Stewart, Anthony. "Vulgar Nationalism and Insulting Nicknames: George Orwell's Progressive Reflections on Race." *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.145-159.

Stone, Oliver, director. *The Untold History of the United States: Episode 2- Roosevelt, Truman & Wallace*. Ixtlan Productions, Showtime Networks. 2012.

Stoycheff, Elizabeth. "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring." *Journalism & Mass Communication Quarterly*, vol.93, no.2, 2016, pp.296-311.

Taslima, Khan. "It All Ads Up: Silverpush's Technology lets Advertisers Reach the Consumers on Multiple Devices. It Could Disrupt Digital Advertising, but Will Face Stiff Competition From Global Pioneers." *Business Today*, 22 June 2014, pp.106-108.

Teck Wee Chua et al. “Hierarchical Audio-Visual Surveillance for Passenger Elevators.” *MultiMedia Modeling*. Springer, 2014, pp.44–55.

Timoner, Ondi, director. *We live in Public*. Interloper films, 2009.

Toscano, Aaron, A. *Marconi’s Wireless and the Rhetoric of a New Technology*. New York, NY, Springer Science+Business media, 2012.

Tufekci, Zeynep. “Engineering the Public: Big Data, Surveillance and Computational Politics.” *First Monday*, vol.19, no.7, July 2014, pp.3-37.

Vaghasiya, Nilav et al. “Mobile Based Trigger System Using Near Ultrasonic Waves.” 2018 International Conference of Smart City and Emerging Technology (ICSCET). 5 January 2018, Mumbai, India, 2018, pp.413-419.

Valenzise, G. et al. *IEEE International Conference on Advanced Video and Signal Based Surveillance*, IEEE, 2007, pp.21–26.

Velden, Lonneke van der. “Leaky Apps and Data Shots: Technologies of Leakage and Insertion in NSA-Surveillance.” *Surveillance & Society,* vol.13, no.2, 2015, pp.182-196.

Vu, V. et al. “Audio-Video Event Recognition System for Public Transport Security.” *Proceedings of the Institution of Engineering and Technology Conference on Crime and Security, IEEE*, 2006, pp.414–419.

West, Sarah. “Data Capitalism: Redefining the Logics of Surveillance and Privacy.” *Business & Society,* vol.58, no.1, 2019, pp.20-41.

Williams, Ian. “In Defense of Comrade Psmith: The Orwellian Treatment of Orwell.” *George Orwell: Into the Twenty-First Century*, edited by Thomas Cushman and John Rodden, Routledge, 2016, pp.45-62.

Winkler, Thomas., Rinner, Bernhard. “User-Centric Privacy Awareness in Video Surveillance.” *Multimedia Systems*, vol.18, 2012, pp.99-121.

Wylie, Christopher. “Fashion Models and Cyber Warfare.” *YouTube*, uploaded by The Business of Fashion, 29 November 2018,https://www.youtube.com/watch?v=IE5ZvAj5tVI. Accessed 24 May 2021.

Zajdel, W. et al. “CASSANDRA: Audio-Video Sensor Fusion for Aggression Detection.” *Proceedings of the IEEE International Conference on Advanced Video and Signal Based Surveillance, IEEE*, 2007, pp.200-205.

Zeppelzauer, Matthias et al. “SoniControl-A Mobile Ultrasonic Firewall.” *MM ‘18*, 26th International Conference on Multimedia, 22-26 October 2018, Seoul, Republic of Korea, 2018, pp.1250-1252.

Zittrain, Jonathan. “Facebook could decide an election without anyone ever finding out.” *Newstatesman.com*. www.newstatesman.com/politics/2014/06/facebook-could-decide-election-without-anyone-ever-finding-out. June 3, 2014, Accessed on April 3, 2021.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* First Edition, New York, NY 10104, USA, PublicAffairs Hachette Book Group, 2019.

Zuboff, Shoshana. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology,* vol.30, 2015, pp.75-89.