A Critical Essay On Today's Technologies Of Surveillance And How They Are Socially and Ethically Used.

Hermione Khan

Introduction

The growth of surveillance technology innovation in the last century is largely unnoticed by the public eye. Innumerable amounts of people across different borders do not realise how, where and for whom their personal data is being used. In 1992, Gilles Deleuze insinuated in 'Postscript on the Societies of Control' that every interaction is measured and quantified, suggestively through the use of surveillance, which accumulates to a society of control, hidden in a pretence of discipline. This hidden society of control which Deleuze depicts has been exposed to the public conjunctively in wide and concentrated ways throughout history, most modernly in June 2013, when Edward Snowden, a former CIA analyst, revealed himself as the whistleblower that exposed the N.S.A's practices of routine surveillance to global news outlets (Dijck, 2014). As Jose Van Dijck states in 'Surveillance & Society: Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology, 2014': "Snowden's disclosures have been more than a wakeup call for citizens who have gradually come to accept the 'sharing' of personal information". This statement by Dijck pinpoints how people have no caution about where their digital metadata is being stored and who has access to it, in a world where social media; online accounts and digital sharing are not only accepted, but expected. Dijck further states that "social networks also - willingly or reluctantly - share their information with intelligence agencies". This leaves one question for the public to consider: If the world's governmental intelligence agencies have access to our metadata, what do they use it for?

In this essay, three case studies will be used to analyse how state surveillance, where surveillance is undertaken by governmental organisations, use technologies to collect quantified data on their populations. These examples include XKEYSCORE, a surveillance program used by the N.S.A (America's National Security Agency), China's phone tracking technology that targets ethnic minority groups and the 'myopticon' of Denmark's asylum system. I will also discuss the social and ethical issues that these forms of surveillance raise and how this contributes to a society of control as suggested by Deleuze.

Case Study 1: State Surveillance Program XKEYSCORE In Conjunction With The Origins Of Surveillance

The 'Datafication' according to 'Big Data; A Revolution That Will Transform How We Live, Work, And Think' (MayerSchoenberger, Cukier, 2013) of mass surveillance techniques using computer systems, like ones Snowden recently exposed, is the "transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis". This acknowledges that every click, search and update is tracked, recorded and turned into a value for governmental intelligence to analyse. This is the sole purpose of the N.S.A surveillance program XKEYSCORE: a computer system used to search and analyse global internet data for the N.S.A to use as evidence against illegal systems and individuals. A 2008 XKEYSCORE training presentation acquired by The Guardian in 2013 suggests that this metadata, collected from any of the 150 global servers that the N.S.A has access to, can

be used to pinpoint an individual's real-time location without their knowledge or consent (De Leon, 2021). In light of this exposure, and many others connected to Snowden's 2013 leak, society began to acknowledge the 'datafication' of their online presence, subsequently growing concerned for how ethically reasonable this practice is when individuals have not consented to the uncovering of their private lives.

The ethics of surveillance has been a disputed topic since its earliest forms within mankind. As Keith Laidler dictates in his book 'Surveillance Unlimited: How We've Become the Most Watched People on Earth, 2008' "spying and surveillance are at least as old as civilization itself". Laidler extrapolates that the rise and fall of empires all relied on knowing the moves of enemies and the loyalty of their populations. From this, one can reasonably suggest that surveillance is at the core of organised civilization and as a result, modern surveillance techniques such as XKEYSCORE may be argued as a 'necessary evil' as former president Barack Obama implied in his response to the exposure of N.S.A practices in 2013: "citizens cannot expect a hundred per cent security and a hundred per cent privacy and no inconvenience" (Dijck, 2014). Deleuze's argument, in this example, is correct: modern technology like that of XKEYSCORE's advanced computer system allows for a wide reach of global activity, therefore allowing the N.S.A to have a sufficient level of control over international society.

What Deleuze's argument fails to highlight is whether these forms of surveillance, however ethically reasonable or unreasonable they may be, create a positive or negative society of control. The N.S.A has access to an abundance of global resources: GCHQ in the UK, Google, Facebook and DSD in Australia, that holistically share metadata for more efficient data collection. While the N.S.A's methods can be seen as invasive and overpowering, they are hidden and inaccessible by contemporary society. This reduces the perception of control that the N.S.A has; the effect of monitorisation not reaching those who search on Google and scroll on social media each day. This concludes that, according to Deleuze's argument, XKEYSCORE contributes to a society of control, where the public is monitored while not being directly influenced by the N.S.A. This form of mass data collection and 'datafication' can be seen as ethically unreasonable, however, its effects are mostly never felt among ordinary citizens as XKEYSCORE's purpose is to target illegal activity. Therefore, it can be seen as contributing to a positive society of control where society is protected and monitored for its own restitution. Some individuals will disagree with this conclusion, however, whether XKEYSCORE has a positive or negative effect, it comprehensively contributes to a society of control enabled through surveillance technology.

Case Study 2: An Investigation Into China's State Surveillance By The New York Times

Comparatively to Case Study 1, the New York Times recently published an in-depth investigation into specific surveillance technologies the Chinese government uses as routine monitorisation called 'Four Takeaways From a Times Investigation Into China's Expanding Surveillance State' (Qian, Xiao, Mozur and Cardia, 2022). The article firstly evaluates that "the Chinese government's goal is clear: designing a system to maximize what the state can find out about a person's identity, activities and social connections, which could ultimately help the government maintain its authoritarian rule". Secondly, it describes "four revelations" which include: the Chinese police analyzing human behaviours to ensure facial recognition cameras capture as much activity as possible, authorities using phone trackers to link

people's digital lives to their physical movements, DNA, iris scan samples and voice prints being collected indiscriminately from people with no connection to crime and lastly, the government wanting to connect all of these data points to build comprehensive profiles for citizens, which are accessible throughout the government's systems and affiliations. It is clear that each of these focused surveillance techniques adds to a larger holistic approach of monitorisation to create a state-wide society of control as Deleuze warns in his argument. Compared to XKEYSCORE, the techniques of surveillance that the Chinese government are implementing and actively testing invade people's private lives and even personal data, not only causing concern in the present but also posing the question of how far they would go in the future to achieve an efficient authoritarian rule, as the New York Times suggests.

The first revelation the New York Times exposed is "police strategically chose locations to maximize the amount of data their facial recognition cameras could collect". This enables the government to store and collect large quantities of facial recognition data that "feed data to powerful analytical software that can tell someone's race, gender and whether they are wearing glasses or masks". According to the investigation, 2.5 billion facial images can be stored at any given time, which approximately equates to 1.8x the population of China itself. The scale at which this data is being harvested supports the New York Times' claim that the Chinese government is using surveillance technology to help maintain its authoritarian rule, as the capacity for storing facial recognition data exceeds the amount needed for country-wide surveillance.

The second revelation of the New York Times investigation includes devices known as 'WiFi sniffers' and 'IMSI catchers' that harvest information using public and private wireless networks, in order to analyze the digital traffic of the phones connected to them, allowing the police to track a target's movements in a populated area. The New York Times described this technology as "a powerful tool to connect one's digital footprint, real-life identity and physical whereabouts". The potential danger this technology could impose is highlighted by the New York Times investigation, as "the police from a county in Guangdong bought phone trackers with the hope of detecting an Uyghur-to-Chinese dictionary app on phones. This information would indicate that the phone most likely belonged to someone who is a part of the heavily surveilled and oppressed Uyghur ethnic minority". The concern about the treatment of ethnic minorities in China, especially the Uyghur population in Xinjiang, Northern China, is a heavily pressing topic in international news media. According to an article about the issue, published by the world-renowned media network the BBC, called 'Who are the Uyghurs and why is China being accused of genocide? (2022)' there are around 12 million Uyghurs that live in Xinjiang and follow the Islamic faith, speaking their own language similar to Turkish. Migration data from the past decade has seen a mass, organised migration of China's majority ethnic group moving into Xinjiang, possibly in an attempt to dilute the region's ethnic culture (BBC, 2022).

The wrongful treatment of this ethnic group does not stop at cultural dilution, however, as the BBC states that "several countries, including the US, UK, Canada and the Netherlands, have accused China of committing genocide". This demonstrates that this ethnic group is heavily oppressed by the Chinese state already, and the use of surveillance technology to detect any resemblance of the culture, such as the previously mentioned Uyghur to Chinese dictionary app, threatens to detect and eradicate this culture altogether. Deleuze only goes as far as to state that digital technology creates a society of control, while in this case, the

interactions surveilled by the Chinese government are leading to a society of oppression and persecution. It is fair to conclude from this revelation that surveillance technology does not only measure and quantify human interactions and activity, but also detects differences in human lifestyle, allowing the Chinese government to detect any individual who does not conform to their authoritarian values upon inspection in this example.

The third revelation expands on previous technology that has been developed by Chinese state surveillance, explaining that sound recorders and iris scanners are being attached to the previously mentioned facial recognition cameras to collect voice prints in a 300-foot radius. According to statements from the Chinese police in the investigation, this technology will enable the state to detect criminals at a fast rate, however, the example of who is being targeted by these surveillance technologies does not conform to an international standard of what a ‘criminal’ is; especially as the most targeted individuals are those in minority groups such as the Uyghur.

Conclusively, the fourth revelation is a holistic use of this data collection, with each type of surveillance technology: facial recognition cameras, WiFi sniffers, sound recorders, and iris scanners, all being used to build a digital profile for targeted individuals that governmental organisations and intelligence can access freely across different platforms. According to the New York Times investigation, one of the largest surveillance contractors ‘Megvii’ is actively working to create “software that takes various pieces of data collected about a person and displays their movements, clothing, vehicles, mobile device information and social connections”. This data profile can justifiably be seen as similar to that of profiles in criminal databases which poses the question: How far will the Chinese government go in order to strengthen its authoritarian rule?

Compared to XKEYSCORE, the effect of monitorisation is heavily felt within the Chinese population as their daily movements, attire, online usage and activities are quantified and stored by the central government who make it known that they are watching civilian movement, unlike the N.S.A who operates in semi-secrecy. According to the statistics website ‘Statista’; 31% of Chinese citizens used a VPN within the second quarter of 2017 (2022). While this data may be inefficient to use as evidence because of its collection date, it still indicates that even before this surveillance technology was fully incorporated into the state data collection routine, a large proportion of China’s population used a VPN in order to browse the internet freely. In recent years, China’s digital censorship has been referred to as ‘the great firewall’ insinuating the scale of how much content, global news and social media is out of reach from Chinese citizens. In this example of state control, Deleuze’s statement is highly valid and can be extrapolated to argue that surveillance technology does not only help to create a society of control, but also a society of despotism, where the rights of citizens are ignored and disposed of in order to achieve a higher level of authority.

Case Study 3: The Surveillance Of Denmark’s Asylum System In Conjunction With The Panopticon

While both XKEYSCORE and China’s upcoming surveillance innovation targets a wide, national area of monitorisation, this example of state surveillance focuses on a minute demographic. This study will focus on the Danish asylum system which while being specific, has an overarching and unseen effect on global values. In ‘Enter the myopticon: Uncertain

surveillance in the Danish asylum system' an investigative journal article written and researched by Zachary Whyte in 2011, the conditions of surveillance that asylum seekers endure in Denmark are rendered as uncertain and anxiety-ridden. Whyte uses the derivative 'myopticon' to describe a physically removed concept of Jeremy Bentham's 'Panopticon' and to gain a better understanding of Whyte's 'myopticon' one must first grasp the Bentham's original concept: first proposed by English philosopher Jeremy Bentham in the late 1700s, the Panopticon is a disciplinary concept materialised in the form of a central observation tower placed within a circle of prison cells. From this structure, a guard can see every cell and inmate but the inmates cannot see into the tower; therefore they never know when they are being watched (The Ethics Centre, 2017). This concept is widely used in theories of surveillance, most notably by french philosopher Michel Focault, who expanded Bentham's concept into a metaphorical architecture in which the aligning components of the Panopticon prison can be used to describe other political and economic systems. Focault notoriously calls the Panopticon a "cruel, ingenious cage" (The Ethics Centre, 2017) introducing the idea of 'Panopticism' in which the watcher is never external to the watched: this is the key idea that Whyte uses in his analysis of the surveillance technologies within the Danish asylum system.

Whyte dictates that the Danish Red Cross acts as the central tower: "At the asylum centre, the central administrative hub was the Red Cross office. Access was via a front desk, where residents collected their allowances and came to make requests. Most had very little sense of what went on within". From this comparison, one can argue that technologically, the computer system that holds all of the asylum seeker's individual profiles in numerical and array-like data, is a form of mass surveillance as the information this system contains has the power to detrimentally influence an individual's future. This data is dependent on their status of processing, age, ethnic origin, gender, intelligence level, state of health and even the safety level of the country they originated from.

Additionally to this level of control that is created from numerical scoring, control over asylum seekers is continuously maintained by creating an environment of uncertainty. While the Panopticon creates uncertainty about whether or not a guard is watching an inmate, Whyte's 'myopticon' describes the uncertainty created by being observed: "applicants worried about what it was the central gaze saw when it did observe them" going further to state "asylum seekers were fundamentally sceptical about the system's ability to recognise truth… being squinted at mistrustfully by the authorities suggested to them that nothing was certain". This indicates that the 'datafication' of their experience and vulnerability into a quantified form is an ineffective representation of their requirement for assistance. This mental uncertainty in theory breeds a hopeless atmosphere for those involved, which in turn prevents sporadic and emotion-fuelled rebellion, allowing, in theory, for efficient monitorisation and control.

Conclusively, in this example of state surveillance, the target is a small yet incredibly vulnerable demographic that Denmark's asylum system heavily surveils. The individuals involved with this system have a 'myoptic' experience, as they know they are being watched but worry about whether their surveillance returns a truthful and just result within the 'datafied' asylum system. The use of mass data surveillance, in this case, may inaccurately represent an individual's experiences and self-worth, however, this technological system built on quantified data efficiently creates a society of control as Deleuze dictates, as asylum seekers have near to no power in their own decision of the future. They can only hope that

their circumstantial evidence which has been quantified and repeatedly processed in numerical forms will give them a positive return of panopticism.

Conclusion

In this essay, three case studies have been used to equate Deleuze's argument that digital technology creates a society of control, in which every interaction is measured and quantified. The 'datafication' of human actions has become systematic in modern society as individuals have their own digital metadata, shared on the internet through personal profiles and accounts. Through Snowden's exposure of the N.S.A in 2013, western society came to realise that their digital metadata was never private and that instead, it was used in a multi-national demographical data flow as a form of mass surveillance of online usage.

This security exposure brought us to the first case study: the digital surveillance program XKEYSCORE created and run by the N.S.A. The study of this example brought us to these conclusions: XKEYSCORE as a digital technologic system allows for wide-spread monitorisation of the public and in consequence, allows the N.S.A to have control over the outcome of illegal activities targeted through this system. This can be seen as a positive control over society, as its goal of multi-national safety and protection benefits normal citizens that have no activity to hide. In this way, this case study aids Deleuze's argument, despite its conclusion extrapolating from his original concept.

The second case study of China's expanding surveillance technology and innovation focuses on an investigation by The New York Times. This article dictates four key innovations that the Chinese government use to maintain their authoritarian rule, one of which targets those who are associated with the Uyghur ethnic group. These surveillance technologies: facial recognition, iris scanning and voice recording in public CCTV cameras, WiFi sniffers and holistic data profiles for civilians, strongly affirms Deleuze's argument that digital technology creates a society of control. As concluded earlier when analysing this example, China may use this technology to identify and persecute minority groups that do not conform to a state standard of the ideal Chinese citizen. Compared to XKEYSCORE, this case study highlights how digital technologies can be used in a stronger affirmation to achieve a society beyond control that borders on oppression.

This targeting of minority groups is also seen in the third case study, which specifically focuses on asylum seekers in Denmark and how they are controlled through a 'panopticonnal' system consisting of statistical data and quantified interactions; neither of which can accurately represent the individuals involved in this closed-loop process. This example does not apply to a large scale compared to the initial two case studies, however, this case study effectively demonstrates the level of control that Deleuze initially hypothesises: The persons involved in this system have extreme uncertainty and anxiety about their future due to the misunderstanding which the 'datafication' of their experiences may equate to. This uncertainty consequently breeds self-surveillance as individuals do not know how their actions will be measured and will therefore act as obedient and patient as possible. Each case study appraises both different and connecting ethical issues from this use of technology. XKEYSCORE can be seen as breaching user privacy on a global scale, however, as Laidler suggests in his book discussing the relationship between human civilization and surveillance: organised civilization is upheld by surveillance and always has

been since human society began. From this, we can evaluate that non-digital forms of surveillance have been necessary throughout history and that digital technologies enable modern surveillance to be as effective as it once was when the world was less developed.

In evaluation, all three case studies reinforce Deleuze's argument that digital technology enables a society of control through the quantification of activity and interactions. They do this in varying levels of extremity and understanding of Deleuze's concept, in consequence, it is evident through these case studies that digital technology has allowed surveillance to become a dominating foundation of organized modern society. Different technologies are used to surveil a population, and the depth of technology that is used often reflects the values of the state governance involved: the United States uses XKEYSCORE for widespread but hidden surveillance, whereas China uses extreme data capture techniques which the population are aware of in order to ensure society's subduing. Compared to this, the Danish asylum system uses a statistically 'datafied' approach of surveillance in order to make the process as fast as possible upon demand, however, this has serious connotations on mental health and representation. Unequivocally, digital technologies are 'wielded' in order to achieve varying levels of control over society and whether they be 'wielded' as tools or weapons is up to the governing state. There is no doubt that society feels this control even if it is insignificantly small and especially when it makes one feel trapped into acting and behaving a certain way. Digital technology may contribute to a society of control or associated powers, but technology alone does not create control. It is human civilisation that creates its own society and through social and economic systems, control is subsequently created, with or without technology's help.

Bibliography

BBC, 2022
‘Who are the Uyghurs and why is China being accused of genocide?’
https://www.bbc.co.uk/news/world-asia-china-22278037
First accessed: 08/12/22

De Leon, Radhamely, 2021
‘XKEYSCORE Spy Program Revealed by Snowden Still a Problem’
https://www.vice.com/en/article/88nmw4/xkeyscore-spy-program-revealed-by-snowden-is-still-a-problem-watchdog-says
First accessed: 05/12/22

Deleuze, Gilles, 1992
‘Postscript on the Societies of Control’
https://www.jstor.org/stable/pdf/778828.pdf?ab_segments=0%2Fbasic_SYC-5187_SYC-5188%2Ftest&refreqid=search%3A3445f6b89e5e692fe17a5d54f39cbcac
First accessed: 28/11/22

Laidler, Keith, 2008
‘Surveillance Unlimited: How We’ve Become The Most Watched People On Earth’
Available to buy or rent as a book/ebook
First accessed: 28/11/22

Mayer-Schönberger, Viktor and Cukier, Kenneth, 2013
‘Big Data; A Revolution That Will Transform How We Live, Work, And Think’
Available to buy or rent as a book/ebook
First accessed: 28/11/22

Qian, Isabelle, Xiao, Muyi, Mozur, Paul and Cardia, Alexander, 2022
‘Four Takeaways From a Times Investigation Into China’s Expanding Surveillance State’
https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html
First accessed: 30/11/22

Statista Research Department, 2022
‘Leading markets for VPN usage among internet users worldwide as of 2nd quarter 2017’
https://www.statista.com/statistics/301204/top-markets-vpn-proxy-usage/
First accessed: 09/12/22

The Ethics Centre, 2017
‘Ethics Explainer: The Panopticon’
https://ethics.org.au/ethics-explainer-panopticon-what-is-the-panopticon-effect/#:~:text=The%20panopticon%20is%20a%20disciplinary,not%20they%20are%20being%20watched.
First accessed: 01/12/22

The Guardian, 2013
‘XKeyscore presentation from 2008 – read in full’
https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

First accessed: 30/11/22

Van Dijck, José, 2014
‘Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology’
https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication
First accessed: 28/11/22

Whyte, Zachary, 2011
‘Enter the myopticon: Uncertain surveillance in the Danish asylum system’
https://www.jstor.org/stable/27975444
First accessed: 12/12/22