The Text, Vol.3, No.2. (July 2021)
ISSN: 2581-9526

Confronting Digital Kleptocracies and Surveillance Capitalism: Analysing the Silicon Valley Fictions *After On: A Novel on Silicon Valley* and *The Circle*

Amal Roy
II MA English Literature
Loyola College, Chennai
Tamilnadu, India

Abstract

The paper will attempt to analyse the working dynamics of surveillance capitalism, which effectively uses the user data, collected without knowledgeable consent from the digital users. The data, which is one of the most valuable resources on earth is then used to manipulate the consumer choices of individuals, thus converting them into products that benefit the capitalists. The paper will also emphasize and draw real life parallel to the fictional constructs portrayed in the primary sources, so as to delineate that the science fiction dystopian nightmares are no longer a fictional entity, but a contemporary reality.

Keywords: Surveillance Capitalism, Privacy Policy, Data Rights, Digital Kleptocracies, Consumer choice.

Introduction

Technology and the Internet have become the two most formidable, influential and powerful forces of the contemporary age. They have become inextricable parts of life and more often, the digital presence of an individual plays a crucial role in defining and determining their existence. The technological world in the last decade witnessed several innovations which led to its exponential expansion, thus triggering the need for frequent updates and upgrades to replace outdated products or software. The trend, as witnessed in the last decade is directly proportional to the increase in the number of digital gadget users. (Palandrani and Little, 2020). Frank Feather, a futurist and a consultant with StratEDGY, opined in a study conducted by Pew Research Centre that Digital gadgets, technologies and the internet have almost become natural extensions of human species and have been integrated into the lifestyles of individuals (Stansbery et al. 2019). The internet-driven society and lifestyle of contemporary times, depends on one powerful, essential and valuable asset, Data. On May 6th 2017, *The Economist* published an article titled, “The World’s Most Valuable Resource is No Longer Oil, but Data.” Since then, it has been widely acknowledged that Data is the new oil, thus underlining its prominence and value in the current economic system. The current economy is even called "Data Economy" which suggests that data is heralding a new revolution in the global economy. The global economy is dynamic and any changes to it create a ripple effect that affects not just the flow of goods on an international scale, but also the lifestyle of people. Trends in the global economy have the potential to influence the career choices and even the lifestyle choices of individuals. The shift to the digital way of life and the technological boom has made data one of the most valuable assets.

Till a decade back, data generated by digital users were mostly considered gibberish and worthless to a larger extent. But with the advent of Big Data, Data Science, Distributive Computing, Parallel Computing and Data Analysis became a mainstream activity that started making meaning and economic possibility of the largely untapped reserve of data. The real potential of data was realized when it was organized into relevant and related databases. The analysed and categorized data has the potential to generate a huge amount of money as the current economy is modelled on it. An important thing about data is that it is infinite. It is being continuously produced and extracted at an exponential rate. Studies have found that human beings produce an astronomical 2.5 quintillion bytes of data on a daily basis. Adding to it the fact that data is always reusable at any time, its relevance becomes perennial.

Whenever users log into the internet and use any social media or other sites, they leave behind digital trails or digital breadcrumbs and it is these trails that are being converted into valuable data assets and sold to the advertisers. Highly intelligent algorithms have been developed by Google and Facebook which accurately predict human behaviour by analysing the data available on an individual by monitoring their digital activities. The process of harvesting and analysing data at a large scale is possible because of the economic model of surveillance capitalism.

1.1 Surveillance capitalism

In the most lucid terms, surveillance capitalism can be described as a data-driven capitalist economic model that uses data, which is analysed and eventually monetized to gain profit. Shoshanna Zuboff in her revolutionary work The *Age of Surveillance Capitalism: Fight for a Human Future at the New Frontier of Power* describes surveillance capitalism as "a new economic order that claims human experience as free raw material for hidden commercial practices extraction, prediction and sales." She also calls it a "parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioural modification" (Zuboff, 2019, v). Capitalism is an economic system that is driven by profit and profit generation is key to the success of any economic system. In surveillance capitalism, the raw material, the data is generated without any initial monetary spending. The collection of data happens mostly without the knowledge of the user. Google and Facebook know more about an individual than anyone else. Their algorithms are so sophisticated and enhanced that they can predict the behaviour of the targeted user from the data that has been collected about them with astonishing accuracy. Revenue flows in through the targeted advertisements designed by the algorithms as they enable the tech giants to advertise and eventually persuade the users to buy or subscribe to the service which is being advertised. Thus, the users themselves become the raw material in a surveillance capitalist society.

1.2 Digital kleptocracy

Amidst all the talk about 'privacy being a myth' in the technology driven world, it is still undeniable that a person's data is their private asset. While the users agree to share their data with software and apps (most of the time not knowing what they are sharing), they are agreeing to give their data for free to the big companies, who in turn generate billions of dollars by selling the users to advertisers, like how Facebook and Google have done. The whole system of selling the user data which are procured by surveillance capitalists free of cost, is the quintessential specimen of digital kleptocracy. According to the Merriam-Webster Dictionary, kleptocracy means, "Government by those who chiefly seek status and personal gain at the expense of the governed." Digital kleptocracy is where a company or a corporation uses the data available at their disposal (most of it harvested from the users without their knowledge) to gain private profit. On the surface, there seems nothing problematic in this economic system. But on a closer analysis, it is understood that the most sophisticated surveillance and personalised targeting systems are employed to harvest the data from the users. The very same data that is collected from the users freely, is used to manipulate and later modify and persuade an individual's behaviour into purchasing the service or product which is being advertised. The manipulative power of surveillance capitalism is strong and persuasive enough to make the personal choices the post-modern society offers look like a facade, orchestrated by the super-intelligent and personalised algorithms developed by tech companies which eventually succeeds most of the time in modifying the behaviour of the individual it targets.

The Cambridge Analytica Scandal (CA) of 2017 was a global incident that threw light on the lengths of data breach surveillance capitalism could inflict on society. Cambridge Analytica, by using the data they collected from Facebook ran political campaigns all over the world and put into effect the mechanics of behavioural modification which eventually succeeded in influencing the voters to cast votes in favour of the candidates endorsed by Cambridge Analytica. CA used targeted advertising campaigns to manipulate the voters, which was powered by the data they procured from Facebook. The economic, cultural and capitalist order of surveillance capitalism is capable of threatening the democratic framework of modern society and the Cambridge Analytica scandal stands as a proof of this claim.

1.3 Primary Texts

The primary texts chosen for the dissertation are *After On: A Novel on Silicon Valley*, written by Robert Reid and *The Circle*, penned by Dave Eggers. Both the novels talk about two different Silicon Valley giants, who use their prowess and influence to extract user data and exploit them. Circle Corporation and Phluttr (the two companies) function as an omnipotent force that employs surveillance to collect data and eventually control the life of their users by manipulating and influencing them. The locale of the novels are set in Silicon Valley, alluding to the power and influence exercised by the real life Silicon Valley. The primary texts also throw light on how big a menace these surveillance capitalists are to the socio-political world order and emphasizes on the need for data rights.

2. Privacy Intrusions and Privacy Policies in *After On: A Novel on Silicon Valley*

In the digital age, privacy has become an entity that is no longer sacrosanct. With technological advancement and sophistication, there has been an influx of apps and online platforms that provide a variety of services. It is mandatory for these apps to provide “Terms and Agreements" and “End User License Agreement” to the users. Due to the complex usage of language and jargon in these documents, most people do not read the agreements, thus giving access to their data to the surveillance capitalists. The apps, especially Social Media apps that mine data from the users, use it to generate revenue for themselves by selling and re-selling the user data. This act is a breach of trust and intrusion into the privacy of every individual, thus paving way for data leaks and breaches. The novel, A*fter On: A Novel on Silicon Valley* is an example of how literature is attempting to blend in with science, economy and digital crises to throw light on the serious issues posed by the postmodern exploitative behemoth, surveillance capitalism.

Rob Reid paints the picture of Phluttr, the world's first Social Operating System. Phluttr thrives on privacy intrusion and harvests user data mercilessly to generate monetary benefits and also establishes a system of widespread digital surveillance in the name of technology. Phluttr functions in a similar way to which the modern-day Silicon Valley giants like Facebook and Google perform. Like Facebook, Phluttr has also been accused of privacy intrusion in multiple cases. Data breaches occurred at Facebook multiple times, in 2013, 2018, and 2019. (Selfkey 2020).

Crafted and brewed with science fiction elements, the novel draws real-life parallels and presents to the reader an opportunity to fathom the depths of the privacy breach and data mining at the hands of surveillance capitalists. Phluttr, the digitally ubiquitous Social Operating System, is representative of the surveillance capitalist mechanism that thrives on data exploitation.

The first instance of blatant privacy breach is seen in the novel when the three protagonists encounter a person wearing a thick smart glass, similar to the Google Glasses. Google released the first prototype of its smart glasses in 2013 and updated the product in 2019 (Williams, 2020). Danna figures out that those weren't ordinary glasses, but sophisticated ones, where speech recommendations were shown on the lenses for the wearer to see. The lens face-IDs the individual in front of them and retrieves all the digital data about them to give the person wearing the glasses information about the other person. Danna says, "That guy didn't know crap about me… but his glasses were telling him what to say" (Reid 30). These smart glasses have inbuilt voice recognition which when spoken to about specific facts, flashes the answer on the lens. This level of sophistication could only be the brainchild of years of research and a vast database. Kuba adds that "Think of all the pictures of you online. Each tagged with a name… Facebook's been Id-ing faces in photos for years. ID-ing someone through live feed via those glasses won't be harder" (31). This statement points fingers at Facebook, which have been notorious for selling user data without informed consent. The Cambridge Analytica Scam of 2017 saw Mark Zukerberg, the founder and CEO of Facebook being questioned by the US

Congress, where Facebook was accused of giving away the personal data of 240 million US citizens to Cambridge Analytica.

A smart glass with the capability of face Id-ing an individual and drawing data about them from different databases is a value neutral product (33), and is dependent on the user's discretion. It runs on data that is illegally collected from individuals. The real-world Google Smart Glasses also have similar characteristics, though not as sophisticated as their fictional counterpart. Google glasses are wearable computers in the form of eyeglasses. It is capable of functioning as hands-free smartphones, capable of doing basic smartphone functions over voice commands ("Google Glass"). The online services used by individuals, mainly, social media platforms track their digital activities, thus discretely collecting the user data and selling it to the highest bidders.

The protagonist trio's confabulation following the encounter with the strange man with the smart glasses led them to conclude that the only company that is capable of conducting such extensive research and funding the next-generation technology is "Phluttr" (34). Phluttr is the first Social Operating System, an integrated suite of mobile apps, online platforms and other websites (125). It is an umbrella that brings together various online platforms like social media, shopping sites and other useful websites. Phluttr "peppers its users with coupons, breaking news, recommendations, gossips and handy info, all of it surgically targeted to the user's interests, locations and state of mind" (51). Mitchell opines that "Phluttr is the intrusive, immoral, and privacy raping social network on the planet" (51). Being a social operating system with the finest brains in Silicon Valley working behind it, Phluttr's capabilities are vast and profound.

"Phluttr knows us from our browsing activity, photos, videos, phone logs, emails, messages, GPS data and other significant data which we voluntarily gave eternal access to the company without reading fully its "Data Donor Agreement." By mining all these data, Phluttr presents to the world meticulously spun and manufactures view of our enviable lives by updating our status for us with AutoPosts" (35).

A social operating system capable of auto-updating its user's stories or statuses is capable of using their data to any extent possible. "Phluttr's surgically targeted ads do not come in cheap... the biggest-paying advertiser, brand manager, and the spin doctor will ultimately be us" (36). Data is more valuable in the hands of well-funded and resource-oriented corporations like the fictional Phluttr or real Facebook and Google. With their efficient and super-intelligent algorithms and prediction software, surveillance capitalists can influence people, their choices and can even make decisions on their behalf.

The Animotion technology that powers and drives Giftish.ly's algorithms run on "Emotes" or "motes." The concept of motes and animotion, run on the basics of evolutionary psychology (44). Thinking is an exhausting activity as far as the brain functions are concerned as the brain consumes 20 percent of the calories consumed by humans. Therefore, the brain has developed several shortcuts, hacks and patches that enable thinking. Sensitive brain MRI scans have seen these shortcuts in the brain performing their function (45). Motes are the nucleic particles of analysis, which when fed to the computers, function effectively and enable them to function in a humane manner in certain aspects, like in match making. In the words of Ellie Stansilow, the scientist who is the brain behind the mote research, "motes are very brief neural events that unfold in the tiny spaces in the brain… they're the core building blocks of emotional states in humans" (58). There are four basic motes, happiness, surprise, anger and sadness. They mix and form twelve patches in repeating patterns, which run through the mind. When the motes are digitally fed into algorithms through analysis, it could evoke consciousness in supercomputers (48). Kuba and Mitchell are convinced that this research suggesting the potential of motes is valid, relevant and possible to be put into effect. If a monetary investment that supports the R&D for the animotion programme were to be funded, Mitchell and Kuba are convinced that they could take the mote programme, which is currently in its childhood stages, to a more advanced level. Though the protagonists are wary and apprehensive about Phluttr's notoriety in privacy breaches and social commitments, to keep their research live and reap benefits for the public, decides to approach Phluttr for the R&D. Eventually, Phluttr and its Phoundr Tony Jepson, realising the importance and applicability of animotion, readily agrees to acquire Giftish.ly, along with the whole team and funds the R&D in animotion technology.

After acqui-hiring Giftish.ly, Jepson the Phoundr, introduces to the trio "Poof", Phluttr's instant messaging service (130) which is used by the employees for internal correspondence. For a company that thrives on privacy violation and data mining, Phluttr has taken great care in making Poof breach-proof. Soon after the message is read by the recipient, it is deleted from Poof permanently and also from all the proxy servers. Moving a step further, it is even deleted from the RAM of both the sending and receiving devices. Important messages have to be memorized by the user as Poof does not provide options to archive them. In short, Poof is a highly secured messaging service developed by Phluttr which covers all the loopholes that prevent a data breach. Drawing real-life comparisons, Poof can be seen as an upgraded version of the "Secret Chat" offered by Telegram or the "Disappearing messages" feature offered by Signal.

Another shock awaits Danna and Kuba, as they learn about the existence of "Philes," from their colleague Tarek. Philes are the entire record of information that Phluttr has collected on an individual and each individual has a specific phile. Phluttr using its privilege, influence and wealth buys databases from different sources. The company buys and stores databases that date decades back from its inception. Phluttr claims that all of it was collected legally. Tarek, to the great surprise of Kuba and Danna, reveals that he happened to see Mitchell's and Kuba's philes, since Jepson, the Phoundr, insisted on cross-checking the Philes of the founders, before acquiring them (137). Kuba is initially devastated and taken aback at this news and considers it as an intrusion into his privacy. Secrets that he believed only he knew, is now on the table due to Phluttr. He realises that Phluttr has more data on him than any spies, Governments or police department has ever had and he is unsettled by the fact. The situation is aggrandized further when Tarek comments that the data on Kuba dates back to his high school days.

Though Phluttr claims that all the data collection is done with proper legal consultations, it is unsettling to know that they have Philes on every individual. Since data is the new oil of the current socio-economic system, amassing databases that hold information about individuals without their consent cannot be viewed in a grey shade. Data mining employed by Phluttr and its blatant disregard for an individual's privacy alludes to the kleptocratic acts performed by Google and Facebook. Digital kleptocracy uses user data to boost their services. Companies like Facebook, Google and even the fictional Phluttr use targeted advertising strategy, where the user data is sold to the advertisers for hefty amounts, thus providing them space to influence and manipulate the consumer choice of the users with pinpoint accuracy. Surveillance capitalists can mine, extract, and sell data because of the lack of stringent data protection laws. Though the world is in the digital age, most Governments are yet to take strong measures to ensure the protection of user data. With strong measures adopted against the kleptocracy of surveillance capitalists, leakage of data, and privacy breaches could be contained to great extents.

2.1 Wingman and its possibilities

A closer look at the smart glass, "Wingman" is needed to know more about Phluttr's current research. It is found that Phluttr has invested half-a-billion dollars (214) in developing the Wingman. Wingman works on augmented reality and writes data overlays on the user's retina (214). This means that, to others, the person wearing a Wingman appears just like a random individual with a cooling glass, but to the person wearing it, a set of apps put information on the retina, depending on the need of the user. In the words of Raj, one of the potential functions of Wingman is navigation. "Tell Wingman that you need to go to Starbucks and it will paint arrows, paintings and directions on the top of your view of the world!"(214).

The application offered by Wingman, which Raj used on Danna when the trio were sitting in a cafe, is named "Slutfinder" (215). Its capabilities are nothing short of technological marvel, but the derogatory name given to the application is abominable. This technology is built upon the data collected from the individuals without their knowledge. "Slutfinder" is a prototype version of a highly sophisticated dating app. It face-IDs everyone that enters the field of vision of the user and filters the prospects, according to the pre-set preferences by the user. It picks the suitable match for the user and does a quick search about the selected prospect and returns with most of the details of the person, thus giving the user of Wingman an upper hand. Jepson argues that everything that Wingman does is permissible from the legal side, as most of the users would have signed the End User Licence Agreement (EULA) of Phluttr, owing to its popularity. The users who install the Phluttr app end up being Face IDed by highly sophisticated technology, capable of pulling out their digital identity for any person who has the financial capability to purchase the product. Using the GPS technology effectively put to use by Uber, Wingman can find out who spent the night with their Tinder date, rather than just texting them. This is possible by tracking their GPS activity in the morning after they met their Tinder date. Capitalism monetizes commodities that have a market value and in the digital economy, no better commodity than data reaps higher benefits than data. It is common knowledge that digital memory is perennial. Surveillance capitalists buy the databases from sources that sell them and eventually, they resell the data, thus creating a loop, which ensures the flow of individual data from one corporation to another.

2.2 Phluttr's EULA

Phluttr's End User License Agreement is notoriously long and complex, filled with legal jargon and written in rigmorolic parlance. EULA's are longer than privacy agreements (339). It is mandatory for every user who opts for Phluttr's service to agree to their EULA. With the acceptance of EULA, the user grants the company access to their data and also gives Phluttr permission to use the data according to their needs. It is to be noted that Phluttr's EULA is a sophisticated trap for its users. Later in the novel it is revealed that most of Phluttr's users agree to its EULA, without even bothering to read or understand it (531). Nevertheless, even if a user reads the entire EULA, "section 2.1.a.iii gives Phluttr the right to change this agreement unilaterally and makes those changes applicable to anyone who uses Phluttr's invasive app or software after the change is made" (237). This means that, even if any user took the painstaking task of reading the entire EULA, they will have to re-read it again every time whenever the company incorporates a change into it.

Probably the most controversial EULA update Phluttr has ever made would be the one where they decided to share the extensive permissions and data they collected under the EULA from their users to their major shareholders (238). Amidst the complex labyrinth of the legal jargons, Phluttr has included the phrase "Assignee In fact via Equity Assignment" (238), by which all the information Phluttr has is shared with their major shareholders. "This includes the right to store, use and resell all the data collected from Phluttr enabled devices" (238). In layman's terms, it means Phluttr's shareholders now have access to call logs, messages, emails, entire GPS history and all the photos ever clicked from Phluttr enabled devices. Even without the user's knowledge, without providing room to make informed consent, Phluttr breaches the trust of its users blatantly and shares their data to third parties. On a closer look at the situation, we can infer that sharing of data to shareholders provides a fertile ground for a data leak.

Shoshana Zuboff opines that "privacy policies or EULAs are considered by legal experts as "contracts of adhesion" as most of them function in a take-it-or-leave-it manner (Zuboff 48). She argues that the "complex nature of the policy documents is deliberately done to discourage users from reading the content" (Zuboff 49).

The Cambridge Analytica Scandal of 2017, had a similar parallel. Brittany Kaiser, a former employee of Cambridge Analytica in her memoir titled *Targeted* makes testimonies to the data breach facilitated by Facebook.

> When people signed to play games such as Candy Crush on Facebook and clicked agree to the terms and services for the third-party app, even without their knowledge, they were opting to give their data, along with their friends' data, free of cost to the app developers and inadvertently, to everyone with whom the app developer had decided to share the information. This data exchange was enabled on the Facebook platform via a data portal called "Friends API." This notorious portal contravened data laws globally… the use of Friends API became prolific, generating great monetary benefits for Facebook… It allowed more than forty thousand developers, including Cambridge Analytica, to take advantage of this loophole and harvest data from Facebook users. (Kaiser 79)

This testimony paints a clearer picture into the activities of Facebook and Cambridge Analytica.

2.3 Data rights in a surveillance capitalist society

Phluttr, as evident from the textual pieces of evidence, is indubitably a surveillance capitalist power. Thriving from user data collected without the proper informed consent of the user, Phluttr uses this data and sells it to the bidders and shares it with the shareholders, providing the ground for a potential data breach. The mass digital surveillance employed by Phluttr by exploiting the nuances of the legal system points to the precise need to have a stringent data protection law, making data rights basic human rights.

The question of data rights has evolved into one of the pertinent questions of the current socio-political-economic world order. Data is the intangible asset of every individual and is the only asset class to which the producers (users) have no rights to its value or any other share of the monetary benefits gained by the surveillance capitalists (Kaiser 375). Stuart Lacey also echoes a similar idea when he suggests that "Personal data is an asset that belongs to the particular individual who has rights on it" (4:42- 4:50). Michael DePalma agrees with the observation of Stuart Lacey when he opines that "Every individual has a legal right and ownership to their data" (14:36- 14:42). Avoiding digital presence on social media might not be the right call to action, as they have become an integral part of the current lifestyle. It is high time that individuals own their data and this is not possible without the systemic support ensured by the governments. When data rights become human rights, the extent to which the users are exploited will be drastically reduced. Individuals should be given the "Right to Forget" where they can demand the tech companies to erase the data the companies have of them. With strict data protection laws, data rights could become a reality and every individual may have a say in who can access their data and determine what happens to them.

3. Digital Surveillance and the Need for Data Rights: Analysing *The Circle*

In the postmodern surveillance capitalist economy, Power lies with the Silicon Valley behemoths, who privately own the lion's share of the free Internet space. David Lyon, a doyen in surveillance studies opines that “The world of today’s surveillance has everything to do with California’s famous Silicon Valley, the incubator par excellence of the digital world that has so rapidly become familiar to so much of the world’s population” (Lyon 10).

This chapter will focus on the novel *The Circle*, written by Dave Eggers. Circle is a Silicon Valley technological and Internet giant that functions as a surveillance overlord, an embodiment of surveillance capitalism. Within six years of its existence, Circle cut a space for itself in the technological industry, by combining woke capitalism with surveillance-based strategies and technologies, in an attempt to create a utopia. To fathom the manipulation employed by Circle, it only takes one to look at their corporate taglines that say, “secrets are lies”, “privacy is a theft” and “sharing is caring” (227). Circle, like Facebook, wishes to make the world more open and transparent. On a closer look at this philosophy, it could be inferred that the purported transparency suggested by Circle is nothing but a “camouflage term for surveillance” (Pignagnoli 152), which strives to create a world devoid of privacy to make it a better place, with the aid of Circle-powered technology and gadgets.

The locale portrayed in the novel is of crucial importance. Most of the events in the plot take place in the Circle campus, which is equivalent to the real-life Silicon Valley. Silicon Valley has evolved from being a hub of innovation and technology to being the seat of power of surveillance capitalism. Circle aspires to create a utopian society that is technologically advanced and transparent. The efficacy of the functioning of Circle Corporation is dependent on surveillance. Every gadget developed by the company and used by its employees are tracked and monitored.

3.1 All perceiving surveillance

The surveillance inside the Circle campus is presented in a sugar-coated way that suggests it as an easy way of getting to know people around the campus and their daily activities, achievements etc. Surveillance is part of the daily routine in the campus and the staff find it as an ordinary ordeal. The posts in the Inner Circle Feed and the Zings (78), perform the role of social media surveillance (David Lyon 13), where the social media users keep an eye on each other. The Circle employees are asked to constantly update their Zings and feeds and also to be social inside the campus. The social media activities and feed updates of the employees are monitored and they are ranked according to their digital activity, thus creating a jovial yet competitive atmosphere to become the most popular Circle employee of the week. This is an effective mechanism to hook people to Circle feeds and constantly monitor their activities, in the name of socialising. In the documentary *The Social Dilemma*, Tristan Harris, former Design Ethicist at Google opines that "Companies like Facebook, Snapchat, Instagram, YouTube and Twitter function on a business model to keep the viewers hooked to their screen" (13:37-13:45). This is very similar to how Circle wants to keep their employees and users glued to their screens. In the later stage of the plot, when Mae decides to go fully transparent (by putting SeeChange cameras on her) all her live feeds, all her day-to-day activities are viewed by the Circle employees through the Zing and they send their likes and dislikes in the form smileys and frowns. By fully being transparent (231), Mae's whole life, apart from her very private moments, is live-streamed to the entire Circle fraternity in a prototype attempt to make the world transparent. Owing to the marketing and campaigning strategy used by Circle, the public demanded the politicians to wear a SeaChange camera and become transparent (181) to bring in honest and accountable politics and lawmaking into the democratic framework of the society.

During a "Dream Friday" meet (48), Bailey, one of the founders of Circle, introduces to the employees what he considers a gadget, a camera which he calls SeeChange (53). It is a tiny camera, the size of a lollipop, powered by lithium battery (50) and could capture videos, images and audio and project them at high resolution. It transmits images and audio through satellite. Owing to its small size and wireless transmission, it is easy to install. Bailey had personally installed it on beaches to demonstrate to the audience the capability of the cameras. Since it feeds live streams, the audience was capable of seeing real-time video through the camera. Furthermore, Bailey explains other utilities to which the cameras can be put to use. By quoting the human rights issues, Bailey hooks the audience and explains that with SeeChange cameras installed everywhere in the globe (he has already installed them around the world, especially in totalitarian regimes) crimes against human rights could be prevented, totalitarian regimes could be kept under check and everything that happens around the globe could be made known to all people. Adding to its appealing factor, Circle, in a couple of years will make the SeeChange cameras available to the general public for $59. Though this sounds utopian, it has a real-life parallel. Gadgets like ‘DropCams’ are easy to install cameras released in the name of stopping crime, but eventually put to use for violating the privacy of individuals (David Lyon 189). The SeeChange camera, despite its utopian vision, is fully capable of creating anarchy in the real world where every random person installs the cameras to stalk, breach the privacy of individuals, thus endangering the current social order of living. No one in the Circle is bothered about the potential misuse of the SeeChange cameras and are transfixed by the speech made by Bailey, thus testifying that in a world dominated by Circle gadgets, no individual is capable of foreseeing the danger of their technology.

Another instance of privacy breach and intrusion that Mae experiences is while she receives an invite to the Portugal brunch on the campus. She believes that the invite must have been sent to her by mistake as she has no connection with Portugal. Annie, her friend explains to her that, since Mae had visited Portugal and stored the pictures she took from Lisbon in her laptop, it is already on the Circle cloud, as the laptop and systems of the employees are automatically connected to the cloud, all the information in the system is uploaded to the cloud. Whenever a need arises, a simple search would return the desired information about the staff. In this case, Alistair ran a simple search to find out the people who have been to Portugal or have some connection to the country. Since Mae’s laptop contents are already on the cloud, the search returned her name and thus the invite (86). Shockingly, Mae seems okay with this blatant intrusion into her privacy and takes it for the normal way in which the Circle works. A world where the personal contents of an individual from their digital gadgets are available to random people on simple search points to the potential dystopia which could be induced by surveillance capitalism.

During another “Dream Friday” meeting which came after Mae started dating Francis, another experience of surveillance induced privacy breach awaited Mae in the form of an app called “LuvLuv” (93), which was introduced to the staff in that meeting. It could be seen as a sophisticated and upgraded version of real-world dating apps like Tinder, Bumble, Grindr, Zoe, etc. LuvLuv also functions on data collected from the users, mainly by employing surveillance and analysing their social media profiles. It uses “high powered” and “very surgical search machinery” (93) to find out more about the romantic interest of a person after a match is made in the app. The app is capable of returning relevant searches to the queries and gives the user a good understanding of the likes, preferences and dislikes of their romantic interest. To Mae’s great horror and embarrassment, Francis volunteered to try the app on stage. He told Gus (the developer of LuvLuv) to search about Mae’s allergies, LuvLuv returned with plenty of answers, all by analysing Mae’s social media posts, her purchase history and her random comments on Facebook. Since Circle purchased all of Facebook’s archives, all the information that was there with Facebook is now at the disposal of Circle’s search engines and algorithms. Aggravating Mae’s embarrassment, Francis continues to initiate searches on her. The searches returned her favourite restaurant and even revealed what items she ordered, by analysing her payments made through TrueYou account. This digital manoeuvre continued and every single time LuvLuv returned the search with accurate responses, all by analysing Mae’s digital activities (96). The accuracy of LuvLuv searches could be attributed to the gigantic database owned by the Circle, as a result of their wide-scale surveillance and capital investment. In the name of dating, a simple app is capable of analysing the whole social media account of an individual, along with their other digital activities. In the world where Circle is present, this might be admired as an innovation marvel, but in the real world, this would generate widespread chaos and cringe among the users. Though not a direct parallel, the Cambridge Analytica scandal also revealed a similar incident of user information being used for nefarious purposes. Cambridge Analytica used the Facebook user information collected via the Friends API platform to draw out voting patterns and preferences of US citizens, (as mentioned in the previous chapter) thus influencing the US Presidential election of 2016.

The tagline of the company itself, though appears utopian and progressive, is an inherent business strategy to promote their brand and services. When Circle says, “privacy is theft”, “secrets are lies” and “sharing is caring” they are not just corporate taglines, it is an attempt to create a support base for the activities initiated by the company. For a company that thrives on surveillance-based technology, it is essential that people see it not as surveillance but as versatile ways to make life better. When the real agenda is camouflaged and presented in a positive light, people welcome it without any inhibitions or premonitions.

Francis works on one of the coveted projects in Circle, named “ChildTrack” (68). Explicating the concept behind ChildTrack, Francis says to Mae that a few years ago, Denmark tried inserting chips in into the wrists of children in a medically sound manner, thus allowing the parents to know where their kids are 24*7. The parents loved this technology and there were no objections to it. It was hailed as an effective way to curb child abuse and child kidnapping. One day, 7 kids were kidnapped and the police followed the trail of the chip and found them in a parking garage, covered in blood. The bodies of the children were found a week later with their wrists slit open (68). ChildTrack takes this technology one step further and in an attempt to make it foolproof, installs the chips into the bones of children. Thus ensuring that it cannot be separated from the body. Francis argues that by installing chips onto the bones of the children, all the child abuse, child kidnapping and other violence against children will be reduced to 99 per cent. Whenever a child is in a place where he/she is not supposed to be, an alert goes off and the parents immediately know where their child is. Thus the surveillance powered ChildTrack technology brings relief to the worried lives of the parents. This is how Circle markets ChildTrack technology. On the surface, this might appear as an astounding achievement, but on a closer look, agreeing to implant a technologically powered surveillance device onto the bones of a child in itself is a controversial act.

The clarion call to make the world more transparent by installing SeeChange cameras on individuals, installation of SeeChange cameras around the world and all other Circle powered technology are instances of woke capitalism put to effective use to sell surveillance capitalism. Installing SeeChange cameras onto the individual, thus making their life an open book to whoever has a TrueYou account is presented as an attempt to make the world more transparent. People are brainwashed into believing that sharing their lives and making them transparent is the only way to make the world a better place. What people might forget is that all the data that is being shared, all the lives that are being made transparent, are being carefully monitored and stored by the Circle servers, thus making them more powerful than any governments in the world. When Google, Tinder, Facebook, YouTube etc. asks for personal preferences to make their services more customized and personalized for their users, it might appear as a genuine attempt to make the user experience better. On the other hand, it is also an attempt made by these surveillance capitalist forces to gather personalised information from their users and use this data to boost their algorithms for targeted advertisements. Thus manipulating the consumer choices.

3.2 Whistleblowers in surveillance capitalist societies

In a digital surveillance powered world, where the chords of control are in the hands of surveillance capitalists, coming out to the public and being a whistle-blower might probably be one of the bravest acts. Only through the testimonies made by the whistleblowers did the world come to know about the extent of surveillance employed by both the state and surveillance capitalist powers. Julian Assange and Edward Snowden are examples.

Another controversial revelation was made by Brittany Kaiser against Cambridge Analytica in 2017. Kaiser, a former employee of the company testified in front of the U.S Congress and Senate, that CA played a crucial role in manipulating the electoral result of the 2016 U.S presidential election. This instance can be seen as an appropriate example that demonstrates the prowess and capabilities of surveillance capitalist power. Kaiser testifies that CA functioned on the data that was purchased from Facebook. Facebook was the main platform through which individuals were targeted. Analysing the data points available on them, CA made personalised content with surgical precision that appeared on the feeds of the individuals, thus influencing them into voting for the candidate for whom CA worked. The social media activity and targeted advertisements employed by CA paid off and eventually Donald Trump was elected president.

Influencing the consumer choice of an individual is one of the effective things that surveillance capitalism does. As evident from the Cambridge Analytica scandal, if the data of the users are analysed using the right tools, surveillance capitalists are also capable of influencing the voting choice of an individual, thus influencing the elections, which in turn would give these companies power to decide who should rule a country. This is not a dystopian vision nor a nightmare from any science fiction novels, this is the reality. Even if an individual willingly shares his/her data with these companies, no ethical code of conduct nor any legal measures binds them to protect these data. As Kaiser quotes, "...theirs was a modern-day dictatorship" (336). Surveillance capitalists like Facebook have not just allowed the user data to be taken away by the highest bidders around the globe, it has also opened up wide possibilities for both foreign and domestic powers to interfere in the elections (336), thus destabilizing the democratic framework of society.

3.3 Data rights, surveillance and democracy

The surveillance society of the current times, empowered by the digital and technological advancements have made Silicon Valley the seat of surveillance capitalism. It might not be possible to live in a world devoid of digital gadgets since human lives are inextricably bound to them. Surveillance capitalism has established itself as a dominant economic and cultural force, hence completely escaping from it is not possible. Acknowledging the fact that surveillance capitalism is an omnipotent force, the best defence against it could be formulating stringent data protection laws as discussed in the previous chapter.

Digital surveillance and surveillance capitalism pose unique threats to any democratic framework. Surveillance capitalists can manipulate people, even without their knowledge thus rigging the electoral process by negatively influencing the voter choices. To avoid this type of data misuse, every individual should be able to own their data and be informed what data about them is being used and who has access to it.

In a landmark turn of events, The Spanish Data Protection Agency upheld the 'right to be forgotten' of the individuals, when it ruled that "all information is not worthy of immortality" (Zuboff 59) and some of them should be forgotten as it is only human. Google challenged this verdict in the Spanish High Court and the honourable high court upheld the verdict of the Spanish Data Protection Agency and asserted that the "right to be forgotten is part of the fundamental principle of the European Union Law of 2014" (Zuboff 59). The Luxembourg Court also seconded the Spanish Court's observation and opined that "though the free flow of data and information is essential, it should never compromise nor degrade the privacy, dignity and data protection of individuals" (Zuboff 59). Adding boost to the claims for data protection laws, and right to be forgotten, countries of the European Union, who have ratified the General Data Protection Regulations (GDPR), opine that the "final say over the digital future lay with the general public and their democratic institutions" (Zuboff 60). Even in a country like the U.S.A, where the private corporations and companies seek refuge behind the First Amendment of the Constitution which guarantees provision for 'permissionless innovation', changes are occurring. In 2015 California's new law asked the operators of online websites and other digital platforms and services to permit a minor who is a registered user of the service to "remove, or to request and obtain removal of content or information posted by the minor" (Zuboff 60,61). These events across the globe suggest that talks for data protection and treating data rights as human rights is going in the right direction, providing a silver lining.

When companies like Facebook provide platforms for other companies to harvest Facebook, Instagram and Whatsapp data of users, it opens the doors for data abuse. Fake news infiltrates the screens of the users, thus making room for manipulated post-truth content to blur the lines of the reality for the users. Being digitally literate and aware of data rights could trigger a possible change towards a better future. As suggested by Dana Budzyn, "consent-based digital platforms should be promoted where the users are in a position to provide informed consent to the service providers regarding data usages so that the service providers are held responsible for their actions" (10:12-10:23).

There might not be an escape from the clutches of surveillance capitalism since it has integrated itself into the current lifestyle of people. The best course of action might be to enforce data rights more concretely and promote digital literacy so that the users know and are informed about their data and how it is used.

4. Conclusion

Surveillance capitalism has shown its potential and capabilities to the whole world. The global economy is data-driven and since surveillance capitalists have access to a lion's share of the user data, they control the economy. A surveillance capitalist society envisions a world where the user data is sold for targeted and customized advertisement which results in the manipulation of consumer choice. If consumer choices can be manipulated, individual behaviours can also be modified, as opined by Shoshana Zuboff (She calls it Behavioural Modification).

Since the world is digitally connected, The Internet has become a giant reserve of information. A world without digital gadgets and the internet cannot be envisaged. Even though the digital gadgets used by people transmit their GPS locations, search histories, preferences, and other digital trails, a life devoid of the internet is not possible. Naturally, then the question of 'what is the alternative,' is to be duly addressed.

Only a few countries in the world have taken privacy concerns as a serious issue. The European Union has perhaps the most stringent of the existing laws and legislations that attempt to safeguard individuals' data from exploitation. Users have started raising concerns about their data that is misused and often exploited by the surveillance capitalists, following the revelations made by Edward Snowden, Brittany Kaiser and many others. These ‘Whistleblowers’ through their activities have made sure that people are aware of the extensive exploitation done by the surveillance capitalists. If gone unchecked, surveillance capitalists are capable of influencing and manipulating world democracies and social order, therefore it is important that Data Rights are considered as human rights. When Data Rights are considered as human rights, exploiting them will be considered as an act of human rights violation. Every individual who uses digital services has the right to know to what extent their data is being used. It is an individual’s right to be informed about the uses to which their data is used, what data is collected from them and who all have access to it. If an individual deems it necessary he/she should be allowed to exercise their “Right to be Forgotten,” where they can ask the digital platforms to permanently delete the data they have on the individual from their server. Surveillance capitalists should be held accountable for the data breach that occurs on their platform and the affected users should be duly reimbursed. It is high time that individuals be given right over their data. Since the Internet giants reap huge profits by selling user data, it is critical that stringent laws be employed to prevent data breach and misuse. It should be made inadvisable and perhaps illegal to write the EULAs and privacy agreements in complex legal jargons. Every individual who uses any digital services should be duly informed in a comprehensible language about the EULAs and privacy agreements, thus providing them room to make an informed consent.

Surveillance capitalism is real and no longer a fictional dystopian entity. Raising self-awareness about its functioning and being digitally literate is very important in tackling the concerns that arise due to this new socio-political-economic-cultural order.

Works Cited

Budzyn, Dana, “Owning Your Digital Self: Monetizing Your Personal Data.” *YouTube,* uploaded by TEDx TALKS, 1 November 2018, https://youtu.be/H27PdSnusCQ.

DePalma, Michael, “Your Data as Property: The Future of Human Rights.” *YouTube* uploaded by TEDx TALKS, 20 July 2018, https://youtu.be/BNCMh6eQcgM

Eddington, Patrick G. “The Snowden Effect, Six Years On.” *Just Security,* 6 June 2019, https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/. Accessed 24 March 2021.

Eggers, Dave. *The Circle.* McSweeney’s Books, 2013.

“Facebook’s Data Breaches- A Timeline.” *Selfkey Blog,* 11 March 2020, https://selfkey.org/facebooks-data-breaches-a-timeline/. Accessed 26 March 2021.

"Google Glass." *WordStream*, WordStream, https://www.wordstream.com/google-glass. Accessed 15 March 2020.

Kaiser, Brittany. *Targeted: My Inside Story of Cambridge Analytica and how Trump, Brexit and Facebook Broke Democracy*. HarperCollins, 2019.

Khan, Shariq. "60% of online users fear unauthorised data collection, only 11% users read privacy policies: Survey." *The Economic Times*, 11 March 2019, https://economictimes.indiatimes.com/small-biz/policy-trends/60-online-users-fear- unauthorised-data-collection-only-11-users-read-privacy-policies-survey/articleshow/68355981.cms. Accessed 20 February 2021.

"Kleptocracy." Merriam-Webster's Dictionary, *Merriam Webster*. https://www.merriamwebster.com/dictionary/kleptocracy. Accessed 18 February 2021.

Lacey, Stuart, "The Future of Your Personal Data - Privacy vs Monetization." *YouTube,* uploaded by TEDx TALKS, 21 December 2015, https://youtu.be/JIo-V0beaBw.

Lyon, David. *The Culture of Surveillance: Watching as a Way of Life.* Polity Press, 2018.

Palandrani, Pedro, and Andrew Little. "A Decade of Change: How Tech Evolved in the 2010s and What's In Store for the 2020s." *Global X*, Mirae Assets, 10 February 2020, https://www.globalxetfs.com/a-decade-of-change-how-tech-evolved-in-the-2010s-and- whats-in-store-for-the-2020s/#:~:text=The%202010s%20were%20a%20decade,shortens%20and%20AI%20algorithms%20improve. Accessed 20 March 2021.

Pignagnoli, Virginia. "Surveillance in Post-Postmodern American Fiction: Dave Eggers's The Circle, Jonathan Franzen's Purity and Gary Shteyngart's Super Sad True Love Story." *Spaces of Surveillance: Spaces and Selves,* edited by Susan Flynn and Antonio Mackay, Palgrave Macmillan, 2017, pp. 152-168. DOI:0.1007/978-3-319-49085-4_9

Reid, Robert. *After On: A Novel of Silicon Valley.* Del Rey, 2017.

The Social Dilemma. Directed by Jeff Orlowski, Performed by Tristan Harris, Hayward, Kara, etc. Exposure Labs and Argent Pictures, 2020. *Netflix*, https://www.netflix.com/in/title/81254224

Stansberry, Kathleen, et al, "Leading Concerns About the Future of Digital lives." *Pew Research Centre Internet & Technology,* 28 October 2019, https://www.pewresearch.org/internet/2019/10/28/5-leading-concerns-about-the-future-of-digital-life/. Accessed 31 March 2021.

"The world's most valuable resource is no longer oil, but data." *The Economist*, 6 May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is- no-longer-oil-but-data. Accessed 17 January 2021.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Public Affairs Hachette Book Group, 2019.