Economic Injustice, Social Conflict, and Surveillance Capitalism: An Exploratory Study of Pakistan

Author

Darakhshan Anjum

Registration Number: 273505

Supervisor

Dr. Ahmed Waqas Waheed

DEPARTMENT OF PEACE & CONFLICT STUDIES

CENTRE FOR INTERNATIONAL PEACE & STABILITY

NUST INSTITUTE OF PEACE & CONFLICT STUDIES

NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY

ISLAMABAD

September 2020

Economic Injustice, Social Conflict, and Surveillance Capitalism: An Exploratory Study of Pakistan

Author

Darakhshan Anjum

Registration Number: 273505

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science in Peace and Conflict Studies

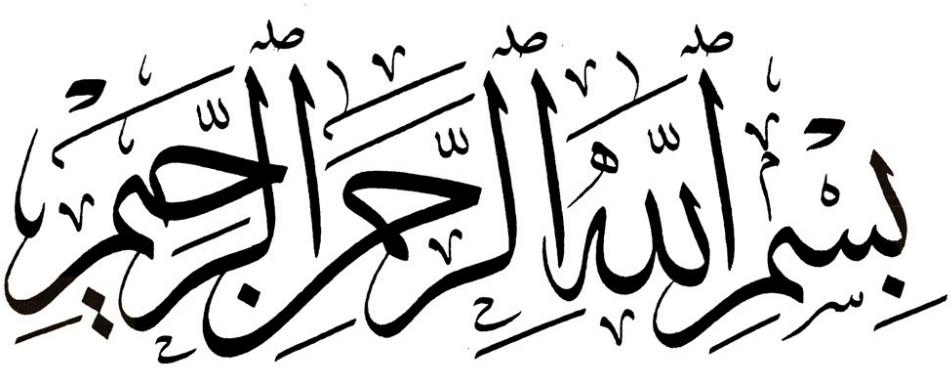
Thesis Supervisor:

Dr. Ahmed Waqas Waheed

Thesis Supervisor's Signature: _____

DEPARTMENT OF PEACE & CONFLICT STUDIES
CENTRE FOR INTERNATIONAL PEACE & STABILITY
NUST INSTITUTE OF PEACE & CONFLICT STUDIES
NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY
ISLAMABAD

September 2020



In the name of Allah the Most Beneficial and the Most Merciful

(We take our) color from Allah, and who is better than Allah at coloring. We are His worshippers.

(AYAH al-Baqarah 2:138)

Al-Quran

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS thesis written by Miss. Darakhshan Anjum (Registration No. 273505), of CIPS (School/College/Institute) has been vetted by undersigned, found complete in all respects as per NUST Statutes / Regulations, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: Dr. Ahmed Waqas Waheed

Date: _____

Signature (HOD): _____

Date:_____

Signature (Dean/Principal): _____

Date:_____

Certificate for Plagiarism

It is certified that MS Thesis Titled "Economic Inequality, Social Conflict, and Surveillance Capitalism: An Exploratory Study of Pakistan" by Darakhshan Anjum has been examined by us. We undertake the follows:

a. Thesis has significant new work/knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
c. There is no fabrication of data or results which have been compiled/analyzed.
d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC plagiarism Policy and instructions issued from time to time.

Name & Signature of Supervisor

Dr. Ahmed Waqas Waheed

Signature **:** _____

DECLARATION

I certify that this research work titled, "Economic Injustice, Social Conflict, and Surveillance Capitalism: An Exploratory Study of Pakistan," is my own work. The work has not been presented elsewhere for assessment. The material that has been used from other sources it as been properly acknowledged/referred.

Signature of Student

Darakhshan Anjum

Registration Number: 273505

COPYRIGHT STATEMENT

Acknowledgments

For giving me space and time to navigate, for refusing to show me the direction but allowing me to find it, for guiding me throughout the journey, for constantly motivating & demotivating me to streamline my thought process, I am thankful to my supervisor Dr. Ahmed Waqas Waheed.

Dedication

To those who read but cannot cohere. To those who see but cannot envisage. To those who hear but cannot listen. To me, to them, to each one of us, the deaf, the dumb, the blind. This is written to embrace irony in life, irony within us. We know we are being watched, used, misused, yet we choose to ignore it. This is dedicated to the ignorance in you & I.

Abstract

A relatively new, precipitously accelerating version of capitalism based on data aggregation has challenged human autonomy and democratic sovereignty. Data is taken from users through surveillance, aggregated into predictive models sold to businesses/governments for profit. This has turned ‘Data’ into the new ‘Currency’. Capital generated through surveillance is just the beginning of the problem. With the surveillance capitalists holding the economic power, and pulling the strings, it has and is leading to economic, and social inequality as well as hampering the electoral system in many countries. The paper draws on Zuboff (2019) work on surveillance capitalism and explores this phenomenon in Pakistan. In situating surveillance capitalism practices as a threat to economic, and social justice, the paper highlights the need for more explicit data protection laws in the country. The danger of surveillance capitalism, the inequalities generated from it, leading to conflict in the society are also discussed.

Keywords: Surveillance Capitalism, data, social inequality, economic inequality, conflict

Contents

Introduction

Context

Privacy, a right to seclude ourselves and our personal information, has become a topic of erudite discussion around the world. Almost every nation has a basic constitutional right to protect privacy. The issue has been debated since antiquity in the form of privacy against gossip, eavesdropping, and later against surveillance, however, it has been the burgeoning of new technology that has turned privacy into one of the frontline global issues (Solove, 2008). At the time when the society just started experiencing an information explosion, Miller (1969) stated that the computer, its voracious hunger for information, its incapability to forget what is stored in it may lead to a disastrous surveillance system that would turn the society into a translucent world. Later, Nock (1993), (Lyon, 2003a), Lyon (2004b), Hoffmann, Proferes, & Zimmer (2018), Gates (2011), Penney et al (2015), and numerous other scholars have explored the relationship between the rise in information technology and the change in the culture of surveillance. Soon after, research was initiated on how the information technology employed for the surveillance of users is shaped by the capitalist imperatives.

Capitalists use surveillance as a tool to control individuals, by employing technologies of information gathering and aggregation. Contemporary capitalism depends on the use of surveillance to reduce uncertainty and enhance the predictability of consumers in the marketplace (Campbell & Carlson, 2002). This emergent phenomenon of surveillance used for capitalism in the online sphere was termed as ‘Surveillance Capitalism’ by Shoshana Zuboff. Surveillance Capitalism uses human behavior as a commodity to generate revenue and has control over the market (Shoshana Zuboff, 2015). This is done at the expense of user privacy. Surveillance capitalists take advantage of the inability of individuals to fully comprehend the potential uses of

their private information (Pal & Crowcroft, 2019). This is a globally present phenomenon; however, this study is limited to Pakistan.

Surveillance in Pakistan is not restricted just to local authorities. Pakistan is the second-most spied country in the world, as per the Snowden revelations (Hussain & Bukhari, 2014). There is an influx of import, export, and procurement of surveillance technologies in Pakistan. With the Pak govt. purchasing deep packet inspection technology from a Canadian company to over 24 government officials being targeted by Israeli spyware company, surveillance is taking place at both national and international levels in Pakistan (Khan, 2019). Surveillance without the consent of the people is in itself, problematic. This problem is aggravated by capitalists using surveillance to generate money leading to the economic and social divide in the country. Thus, it is essential to understand this problem.

Research Questions

Research questions are explicit statements of what it is the researcher wants to find out. The research questions formulation is connected to the existing literature on the subject (Bryman, 2001). This paper using Deleuze & Guattari's (1987) theoretical framework of how corporations are creating societies of control, and Shoshana Zuboff (2015) conceptual framework of surveillance capitalism, argues that surveillance capitalism is a phenomenon present in Pakistan.

The research questions of this study are:

- How Surveillance Capitalism is taking place in Pakistan?
- How Surveillance Capitalism is leading to economic and social inequality in Pakistan?

The concept of surveillance capitalism would be explored, in light of, the law of privacy in the country. The research questions in this study are grounded upon the information already known about the phenomena, and they have a direct relationship with the objectives of the study.

Objectives of Study

The paper aims to explore how the phenomenon of Surveillance Capitalism is taking place in Pakistan. To do so, it would be determined by how the online data of Pakistani users are surveilled which in turn is used to generate capital. This study would ascertain how surveillance capitalism is creating an economic and social divide in the society, between political, economic capitalists, and the general public. Thirdly, this study would discuss the aspect of the risk of conflict in a surveillance capitalist society.

Methodology

This research employed an exploratory qualitative approach to achieve the above-mentioned objectives. Qualitative research is driven by its process orientation towards the world and its inductive approach. The meanings in the research are understood through the lens of the participants in the study (Maxwell, 2013). Through interviews and observations, the point of view of the participant is described (Orb, Eisenhauer, & Wynaden, 2001). The case of Pakistan was taken to explore the phenomenon, thus the research employed a case-study approach within qualitative research to achieve its objectives. Qualitative research typically involves a small number of individuals or situations, like in the current study only 9 participants were interviewed, aiming to preserve the individuality of each of these in their analyses (Maxwell, 2013). An exploratory study, at its core, aims to discover something new. This particular study is exploratory in nature as the concept of Surveillance Capitalism has never before been explored in Pakistan (Swedberg, 2018). There is a sequence in which a qualitative research process is conducted.

The first step is to have a general research question. Qualitative research requires the researcher to have general research questions, that can have a varying degree of explicitness (Bryman, 2001). The research questions of this research were to explore the existence of surveillance capitalism in Pakistan and its repercussions in the form of social, and economic inequality leading to a risk of conflict. On the basis of those research questions, a questionnaire was drafted and questions were asked from respondents.

With this, we come to the second step that is to select relevant site and respondents. The research was conducted on Pakistan as there is a lack of work done on surveillance in Pakistan, as for respondents they were identified based on the research questions.

The respondents of the present study were sampled using non-probability purposive sampling. This type of sampling is done with reference to the goals of the research to allow the research questions to be answered. Also, purposive sampling lets the researcher sample in a way that there is a range in the resulting sample, so that sample members vary from each other in terms of essential characteristics pertinent to the research questions (Bryman, 2001). This was key to this research as there were 9 respondents in the present research and they belonged from different walks of life, and in one way or the other, they had relevancy to the research topic.

Appropriate sample size can range from 6 to 12 participants if the researcher reaches thematic redundancy after hearing the narratives of 6 respondents (Thomas & Pollio, 2002). Similarly, research can have participants ranging from 5 to 25 (Creswell, 1998) or/and there can be a relatively flexible 2 to 10 participants sample size (Munhall, 1989). In this particular research, there were 9 respondents.

The respondents were an expert from the U.S, a cryptography professor, a cybersecurity specialist, a technical analyst, a retired PTA Employee, a bank worker, a NADRA official, Director Research and Policy Digital Rights Foundation, and a present PTA data analyst. The reason for selecting these participants is that either they belong to an organization that conducts surveillance in Pakistan, or they have technical knowledge of how surveillance capitalism is taking place in the country.

The interviews were conducted at different time frames between March to July 2020. The first two interviews were conducted in March before the COVID-19 pandemic hit the country, and most of the country went into lockdown. Thus, only these two interviews were conducted face-to-face. In face-to-face interviews, one aspect pertinent to mention is the interview location. The place of the interview should be convenient to the respondent, private yet familiar to him/her (Gubrium, Holstein, Marvasti, & McKinney, 2012). In this research, the researcher conducted both the interviews at the offices of the respondents.

Four interviews were conducted via telephone. In research terms, a telephone interview is a approach to obtain data that permits interpersonal communication without a face-to-face interaction (Carr & Worth, 2001). The remaining three respondents responded in a written word document which they sent via email. Email interviews allow the researcher to conduct asynchronous interviews. Unlike, other interview forms, respondents can respond to email interviews at their own convenience (Hawkins, 2018). There were a couple of questions the researcher asked the respondents before conducting the interviews.

Before starting every interview, the researcher asked the respondents two questions. The first question was whether the respondents wished to remain anonymous in the study, or their names can be revealed. In qualitative research, anonymity helps in honest disclosure of sensitive

information while protecting the confidentiality of the participants (Given, 2012). 7 out of 9 respondents wished to remain anonymous. Thus, their names will not be mentioned in the present study, only their professions will be stated. Two respondents permitted using their names in the study, thus they will be shared in the respective research.

The second question asked the respondents prior to conducting the interview was whether they would permit voice recording of the interview. Out of 9 interviews, three were in written form thus there was no voice recording. Out of the remaining six, three participants did not permit voice recording of their respective interviews. The remaining three allowed recording of the interview.

The third step in a qualitative research process is the collection of relevant data from the participants. In order to answer the research questions data was gathered from the sample. In this study, semi-structured interviews were conducted for the collection of data. Interviewing gives the researcher access to the observations of others (Gubrium et al., 2012). Qualitative interviewing tends to be less structured as there is more focus on the interviewee's point of you. In this study the researcher framed new questions from the responses of the interviewees' replies also referred to as follow-up questions or probes, thus it was a semi-structured interview.

The quality of an interview is dependent on appropriate preparation, demonstrating respect for interviewees, careful listening amongst other things (Flick, 2018). In this particular study, the researcher prepared a few questions prior to conducting interviews. However, the researcher displayed flexibility in deviating from the earlier plans wherever necessary. A balance was maintained between the authenticity of the research questions and the experiences of the interviewee. The researcher made sure to allow respondents to speak freely and articulate their views on the topic. This was maintained by intensive listening and necessary prompts by the investigator, where needed.

In interviewing there is a power struggle between the interviewer and the interviewee. As interview questions are in the hands of the interviewer, it allows the interviewer to exercise power and control, the topics shift and turns in an interview. However, the interviewee can use their status or answers to challenge and resist following the interviewer's lead. Thus, there is a power struggle between the two parties (Gubrium et al., 2012). In this respective research, every interview was treated differently. Some respondents were more welcoming and willing to answer every question. In such interviews, the researcher controlled the flow of the conversations. These interviews were lengthy as well in comparison to the other interviews. Similarly, the researcher encountered those respondents as well who gave one-liner answers and were uncooperative in their responses. In those interviews, the interviewee channeled the conversation.

The fourth step is the interpretation of the data. For data analysis and interpretation, transcribing the data is the first and most essential step. Transcription requires a deep observation of data through repeated attentive listening. This allows the researcher to get familiar with the data, which then facilitates ideas that emerge during the analysis part (Bailey, 2008). Transcription helps in the identification of key themes and allows the researcher to become aware of the similarities and differences between different participants' accounts. In this study there were a few respondents who did not permit audio recording of the interview, thus the researcher immediately wrote down important details of the interview after conducting it. The rest were transcribed at different points and revisited numerous times while writing the analysis.

In the collection of data, one of the issues that the researcher faced was that of a reluctant respondent. Research gets plagued by the respondents who either refuse or frequently postpone, break appointments, and are indecisive about cooperating or not. These respondents have a dispiriting effect on the researcher (Robins, 1963). In this research, the researcher encountered

many reluctant respondents who first committed to giving interview but later they did not answer back to emails/messages.

The fourth step in the research is the interpretation of data. The interpretation of the data in this research was done using thematic content analysis. Thorne (2000) has called data analysis the most complex phase of the qualitative study. Thematic analysis is a method to identify, manage, explain, and report themes uncovered within a data set (Braun & Clarke, 2006). The thematic analysis uncovers the themes relevant in textual data at different levels (Attride-Stirling, 2001). The advantage of this analysis lies in its ability to examine different perspectives of different participants generating unanticipated insights (Norris & Armstrong, 1999). The themes uncovered in this research were surveillance capitalism, economic inequality, social inequality, law of privacy, and risk of conflict.

Significance

Scholarly work has looked at different dimensions of surveillance capitalism. Shoshana Zuboff has written numerous scholarly articles and a book on how surveillance capitalists are automating us, eroding the process of individual autonomy, putting forward this question that if surveillance capitalism remains unimpeded, what new damaging and regretful bequest will be grieved by future generation. Cinnamon (2017) argued about how the acceleration in surveillance capitalism is threatening social justice. Lehtiniemi (2017) discussed how emerging intermediary services 'Personal data spaces' can be an intervention in the surveillance capitalism model. However, surveillance capitalism is a phenomenon that has not been studied at all in Pakistan. Thus, this study would not just try to explore this concept from the perspective of Pakistan but also open pathways for further studies in this dimension in the country. The study would advance knowledge within the field of Peace and Conflict studies by its analysis of how surveillance capitalism is

enhancing economic, social inequality in Pakistan, which can lead to conflict. This study matters because we live in the times of technology, where power is not just defined by territorial expansion, but more so by the surveillance capitalists.

Limitations

There were two limitations to this study, a generic and a specific one. This study was conducted at a time when the world was/is facing COVID-19 pandemic. The lockdown in Pakistan amidst the pandemic restricted the researcher in conducting face-to-face interviews. It also limited the number of interviews conducted, which if the situation, would have been normal, could have been more. Another limitation, specific to the study was that potential respondents backed off from giving interviews once they got to know the gist of the thesis. Most of them were hesitant to talk about surveillance, and how it is being used/misused in Pakistan, as it is considered a sensitive topic.

Chapter 1: Literature Review

This chapter is divided into three sections. In the first section, the theoretical framework of surveillance is discussed, it is explained which framework is appropriate for the present study and why. In the second section, the conceptual framework upon which this entire thesis is based is conferred. The conceptual framework of the current research is 'Surveillance Capitalism'. In the third section, the empirical evidence is given stating the repercussions of Surveillance Capitalism.

Theoretical Framework

A shift from industrialism to informationalism in the past few decades has transformed the global economic dynamics. Industrialism, prompted by the Industrial Revolution witnessed the growth in materials engineering, and transportation. On the other hand, informationalism, triggered by informational revolution that began following World War II was marked by the development in computer science, electronics, and telecommunication networks (Hardt & Negri, 2000). The technological paradigm of informationalism replaced the previous industrialism paradigm (Castells, Castells, & Manuel, 2004) that led to a movement away from the manufacturing and industrial economy towards information production, accumulation, & processing economy (Cohen, 2016). The initial years of informationalism paradigm specifically the decade of the 1990s witnessed economic globalization. But then, as a result of the September 2001 terrorist attacks, there was an increased need for use of technology in the domain of 'security' that led to the heightened interest in surveillance (Gregory, 2011). Surveillance literally meaning 'watching over' (Lyon, 2010), is an inescapable component of Information Communication Technologies (ICTs). The shift towards informationalism paradigm, radical technological changes brought about since the 1990s, has allowed us to look at surveillance from different lenses.

Surveillance can be understood using different frameworks out of which the most noteworthy one is the panopticon model. Foucault's concept of panopticism (Brunon-Ernst, 2016) looks at Prison, Pauper, Chrestomathic and Constitutional panopticon (Galič, Timan, & Koops, 2017). A constant surveillance illusion is created in prison-panopticon in which the inmates feel that they are being persistently watched by the guard in the central tower, who is perceived as an invisible omnipresence (Foucault, 1979). This established the disciplinary component of the Panopticon that aimed to impart a kind of productive 'soul training' and encouraged inmates to reflect upon the minutia of their behavior in a subtle and continuous effort to transform their selves in prescribed directions (Lyon, 2006). The other three lesser-known Panopticons simply replicated the original Prison Panopticon concept in which the prison is replaced by school, hospital, or/and a factory (Galič et al., 2017). Foucault has provided us with a framework to understand surveillance, but now many scholars have accentuated the limitations of the panopticon for understanding contemporary surveillance.

Panoptical instinct is not fading away but the concept has its limitations, as depicted in the literature. Bauman (1998) states that the panoptic model of 'securing and perpetuating social order' is now obsolete. The model is just applicable in societies in which the inhabitants have fixed places, functions, and appetites contrary to the advanced contemporary societies (Bauman, 1998). Similarly, surveillance is not exclusively directed at the poor and dispossessed anymore, as the panoptic model explained. It is ubiquitous, with people belonging from all segments of the social hierarchy coming under scrutiny (Nock, 1993). Yet another limitation of Foucault's concept of Panopticism is that it is considered unimportant as to who sits in the central tower, as the effects on the subject of surveillance are deemed identical regardless of who is doing the watching (Lyon, 2006) however, Norris & Armstrong (1999) stated that the racial prejudices are apparent of CCTV

operators in disparate scrutiny of specific ethnic groups. Thus, it does matter, who is doing the watching which means that the fixed roles of surveillance operators and individuals are no longer so defined as they were in Foucault's analysis, hence they require a different framework for understanding.

Foucauldian institutions and its ways of disciplining have shifted into other surveillance modes. There is a shift from disciplinary societies to control societies, as observed in the work of Deleuze and Guattari (Deleuze & Guattari, 1987). The idea of discipline as a driving force of governing is dismissed by Deleuze. The institutions of school, hospital, and factory are replaced by corporations and the objective has shifted from maintaining the discipline to having relentless control over individuals (Deleuze, 1992). In Foucault's concept of panopticism, the main aim was to achieve a long-term, stable society through discipline while in Deleuze's controlled society the focus is more on short-term results. For this constant control is required which is achieved through incessant surveillance, market assessment, strategies, etc (Galič et al., 2017). In a Deleuzian society individual's representation become more relevant in comparison to individuals themselves. The divided individual termed by Deleuze (1992) as 'dividual' monitors and controls the purchasing behavior of consumers. The data-bodies of consumers gain value over their real bodies. The individuals are considered entities with many different roles and representations, and not as uniform or complete beings. Deleuze focused on open spaces and surveillance at a distance rather than monitoring just in closed spaces like a prison, factory, or a hospital (Galič et al., 2017). The foundation laid by Deleuze of Post-Panopticism literature was further explored by other surveillance scholars at a time when ICTs became more pervasive.

Building on the work of Deleuze, post-panoptic surveillance was further explored by Haggerty and Ericson. The concept of "the surveillant assemblage" was first introduced by Deleuze and

Guattari (Deleuze & Guattari, 1987) to describe surveillance networks and then further explored by Haggerty & Ericson (2000). The focus was on how the many surveillance systems to which people are exposed decipher the bodies into abstract data. That data is then re-assembled as decontextualized “data doubles” upon which organizations act (K. Haggerty & Ericson, 2000). A rhizomatic leveling of the ladder of surveillance is witnessed so much so that groups that were earlier exempted from routine surveillance are also being surveilled (Bogard, 2006). Hitherto, panopticon, and post-panopticon surveillance literature is discussed, it is essential to substantiate the approach that is more suitable for this study.

Conceptual Framework – Surveillance Capitalism

Surveillance understanding cannot properly commence without the acknowledgment of the sustained influence of Foucault’s panoptic model, however, for this study post-panopticon approach, led by Deleuze is deemed appropriate. Even though, in line with the concept of panopticism, authors like Staples (1997); Lyon & Zureik (1996) defined surveillance as an act of keeping a close watch on people, monitoring of everyday life resulting in collection and interpretation of personal data. This close observation was especially directed towards a suspected person, however now in the contemporary world, better understood by the post-panopticism model, most of the new surveillance technologies are not "especially" applied to "a suspected person" (Marx, 2002). Also, close observation fails to incorporate contemporary practices, as surveillance can be conducted out from far away with satellite images or the remote monitoring of communications (Marx, 2002). Similarly, Foucault’s panopticon understanding did not pay much heed to ‘who’ is watching but post-panopticon work highlights how surveillance is frequently negotiated through human agents and security networks which makes its outcomes context-

specific and exceedingly variable (McCahill, 2002). Thus, different approaches are used for better comprehension of surveillance, with 9/11 resulting in heightening of surveillance.

The September 11, 2001 attacks on New York and Washington triggered immediate reactions, out of which the most noteworthy one was to enhance surveillance. It was believed that the risk of another such attack could only be controlled with a better system in place. Prevention of future such attacks depended upon means of better identifying, classifying, profiling, assessing, and tracking each and every individual (Lyon, 2003a). For this, technological solutions were sought thus the decade that followed 9/11 was a bonanza for corporations that dealt in surveillance technologies (Lyon & Haggerty, 2012). Similarly, the surveillance power of government expanded and it was directed not just at the people suspected of misconduct but at all the citizens (Aas, Gundhus, & Lomell, 2009). It was reported in the New York Times that post 9/11 NSA was sanctioned by President Bush to spy on local calls and private emails without approved warrants from the court (Sinha, 2014). This also led to a paradox. Post 9/11 the paradox was that even though people became more transparent to organizations, the organizations became opaque and veiled in operational secrecy (Lyon & Haggerty, 2012). The organizations, specifically tech companies maintained secrecy in surveillance led by the digital giant ‘Google’.

Google, founded three years prior to the 9/11 incident ensured that the implications of its mission remain unknown. The operations of Google were not easily accessible to the outside world (Hoofnagle, 2009). Apparently, Google’s mission was to open a new world of searchable web pages for its users. However, when users searched online, each Google search query produced collateral data including the number and pattern of search terms, the phrasing of the query, click patterns, spelling, location, etc. This was earlier regarded as waste material or data exhaust. Later on, the company, in disguise started turning the growing cache of this behavioral data and its

computational command and proficiency towards one single task, which was to match ads with the queries. The raw material that was initially just used to improve the search quality was now used for target advertising to individual users in order to generate capital (S. Zuboff, 2019). The commercial power of behavioral surplus was understood by leadership at Google and secrecy was necessary for its sustained accumulation (Levy, 2011). Thus, the users' curiosity was avoided by limiting their exposure regarding any clues about the reach of Google's data operation (Edwards, 2011). This marked the beginning of data-driven service delivery from 'mass-production' towards 'mass predictive personalization' (Yeung, 2018). Google, by secretly using the behavioral surplus to generate capital changed the dynamics of surveillance and became the inventor of what we now call 'Surveillance Capitalism'.

Surveillance Capitalism is an unprecedented market form that uses 'individuals' as sources of the behavioral surplus and enterprise as the customers of the surplus. Zuboff (2019) defines surveillance capitalism as a process in which human experience is used as free raw material for translation into behavioral data. Some of the data is used to improve services, while the rest termed as 'behavioral surplus' is used to develop prediction products that anticipate what users will do now, soon, and later (Andrew & Baker, 2019). It is also used to manipulate user behavior to make predictions more accurate by elbowing them in certain directions (Landwehr, Borning, & Wulf, 2019). This concept of surveillance capitalism is unparalleled in history.

This concept is unprecedented as it is a distinct new actor in history which unlike the common perception, is not an inevitable consequence of technology. It is a logic that permeates technology and leads it into action. Surveillance capitalism does employ many technologies but it is not synonymous with 'technology' itself. It is driven by the puppet masters that have hidden behind the algorithms and machines. They are the political and economic capitalists aiming to use the data

to predict and alter the future behavior of people and sell it to the government and the corporations (S. Zuboff, 2019). This surveillance capitalist market was first explored by capitalists at Google, and later it spread into the cyberspace with Facebook following Google's footsteps.

Facebook was the first and by far remains the most belligerent competitor for behavioral surplus supplies by using surveillance capitalism. Facebook CEO Zuckerberg rejected charging users fees for connecting them together via the app (Hoffmann et al., 2018). So the question was, how to turn the Facebook users into money (S. Zuboff, 2019). They did this by realizing that they have better information than anyone else about users, from knowing their gender, age, location, profession, hobbies, friends, pictures, etc. Here the behavioral surplus was used not just to satisfy demand but also to create it (Kirkpatrick, 2010). The Like Button of Facebook introduced in 2010 was used to place cookies on the computer of a user, irrespective of whether a user actually used the button or not. This allowed Facebook to track, trace, and process user data (Roosendaal, 2012). Detailed profiles of users were built for personalized targeted advertisements (S. Zuboff, 2019). The capital generated was evident as by 2017 the 71% earning surge of Facebook was hailed by Financial Times with the headline, "Facebook: The Mark of Greatness". It ranked 7th amongst the top 100 companies in the first quarter of 2017 ("Facebook muscles its way to 71% earnings surge | Financial Times," 2017) when a year earlier it wasn't anywhere near the top 100. This expansion that started off with Google, spread to Facebook, soon started attracting telecom, cable companies that were determined to compete for the surveillance revenues.

Starting from the largest corporations in the U.S leading to new and established companies from every sector, businesses started shifting from their established fees for service models to monetizing behavioral surplus. The largest telecom company in the U.S, Verizon publicly announced its shift towards mobile advertising in 2014. The company aimed to solve the tracking

needs of advertisers by assigning a concealed tracking number to each of its users (Bergen & Kantrowitz, 2014). Soon after similar tracking IDs became standard all over the telecom industry. Then companies from the retail sector, finance, fitness, insurance, health, education, automotive, travel, etc. shifted towards the surveillance revenues enticed by its humongous growth and profit. Surveillance capitalism was born digital but it was not confined to digital companies only (S. Zuboff, 2019). Companies also started offering surveillance in the interest of behavioral surplus as a service. These companies are often termed as “software-as-a-service” or SaaS but in reality, they are “surveillance as a service,” or “SaaS” and ‘video surveillance as a service’ VSaaS (Neal & Rahman, 2012). Companies like Safegraph partnered with tracking user behavior apps to accumulate data of where users are throughout their day (Jeffries, 2017). The unprecedented success of Google, Facebook, later on, Microsoft, and then any company with an online presence, exerting a palpable magnetism on the global economy brings us to the question of how the government provided shelter to surveillance capitalism.

Those in power especially in the global north played a part in sheltering surveillance capitalism from scrutiny. Initially, in the 1990s, legislations like the 1995 European Union Data Protection Directive, the U.S Health Insurance Portability and Accountability Act ("HIPAA"), and the Children's Online Privacy Protection Act ("COPPA") were passed to address privacy. However, in the aftermath of the September 11, 2001, terrorist attack, focus shifted from privacy to maintaining security (Swire, 1999). Legislations were passed in the US Congress and EU that asserted the need to expand surveillance activities as there was a growing earnestness to know. This created a “state of exception” favoring Google and other tech companies to grow and continue their surveillance-based logic of accumulation, leading to surveillance exceptionalism (S. Zuboff, 2019). Surveillance exceptionalism thrived with state security agencies seeking ways to avail

Google's surveillance capabilities and develop further tools to enhance it. So much so that the U.S intelligence agency even built its own secret Google by launching a pilot project ICREACH that had a "Google-like" search design and enabled analysts to extract important behavioral surplus using volumes of metadata (Gallagher, 2014). Now that the surveillance capitalists got the support of the concerned authorities, they encompassed new unexplored territories, ahead of clicks and queries.

In order to improve predictions and diversify in scope, surveillance capitalists widened their extraction architecture to incorporate new surplus sources. Google became harder to catch than ever by investing extensively in AI, training its own algorithms, launching projects like 'Google Artificial Brain' (Mayo & Leung, 2018), becoming the pioneer of hyperscale, the largest computer network on Earth (Allen, 2019). From January 2014 to Nov. 2016, Google purchased 9 AI startups (McLaughlin & Sullivan, 2017). Google expanded its primary supply chain for behavioral surplus from 'Search' to its Android mobile platform (Gandhewar & Sheikh, 2009). For drawing users into Google Search and other services, sustaining known terrains of behavioral surplus, and opening up new ones, Google licensed Android to mobile handset makers for free (Barr, 2015). Extending its reach, Google, a search company, started investing in smart-home devices, wearables, and self-driving cars while Facebook, a social media network, started developing drones and augmented reality. Similarly, Google became the top contributor in the most prestigious scientific journals in order to promote its own narrative and resist societal apprehensions (S. Zuboff, 2019). As surveillance capitalism expanded, diversified, and spread geographically from the U.S, to Europe making inroads in every region of the world, the technology in itself also advanced towards iris scanning, biometrics, cashless transactions.

Surveillance Capitalists' reliance on technology and advanced tech infrastructure became the core of surveillance capitalism. Technological surveillance post 9/11 improved by incorporation of biometrics, identification (ID) cards with embedded programmable chips, Closed Circuit Television (CCTV), communicational measures like wiretap & web-based surveillance and cashless transactions (Lyon, 2003b). Identifactory and diagnostic data were obtained directly from the body using biometrics and genetic methods (Lyon, 2004b). Biometric technology basically collects the digital representation of physiological features that are unique to an individual, but in essence, it is treating the body as information (Van Der Ploeg, 2005). By treating the body as information surveillance has become an intrinsic part of our daily life, so much so that it is hard to pinpoint how it is changing with time (Misa, Brey, & Feenberg, 2003). Biometrics are often than not, used in smart cards and are implicated in CCTV facial recognition systems as well. As for communicational surveillance, it deals with monitoring behaviors (Lyon, 2003b). Similarly, the daily transactions shifted from cash to credit and debit cards which as per Swire (1999) will allow the user record of each transaction to be created and placed automatically into databases allowing extremely detailed information about the purchasing history of individuals to be revealed. The downside of surveillance capitalism comes in many forms, starting with the erosion of users' privacy.

Empirical Findings – Repercussions of Surveillance Capitalism

Users are concerned about their privacy, but they often try to vindicate these concerns as they are not aware of the extent to which it is misused. Users do not read privacy policies (Groom & Calo, 2011). Even if they did it would take them months even years to read all the privacy giveaways (Pasquale, 2013). Also, as per Radin (2014), the prospects of a user renegotiating the terms and altering them for an intermediary like Facebook or Google are quite low. This has led to a privacy

paradox. Swire (1999) describes it as in the long term, people are concerned about surveillance capitalism leading to the government accessibility to private data while in the short term, as particular user data is at stake many people prefer to let it be rather than trying to withhold privacy values. Adding to the erosion of privacy, is the fear of not knowing where, how, and to what extent the data is being misused. Even the data warehouses, that manage the data have just a general awareness of its future uses (Gandy & Herbert Schiller Professor, 2002). Other than having less awareness about privacy, the free services of Google, Facebook are so appealing that once bitten, the apple becomes irresistible. If you try to totally avoid having an online presence then you become non-existent. Standing afar for the sake of privacy seems like a lonely prospect (S. Zuboff, 2019). Thus, the short-term decision of not to respect privacy overrides the long-term concern for privacy that has its repercussions.

The shortcomings of surveillance capitalism and disregard for user privacy has its consequences, one of them being identity theft. Identity theft is a crime in which personal information of an individual is illegally used to gain benefit (Whitson & Haggerty, 2008). The information is taken using informational profile of individuals which we earlier mentioned as ‘data doubles’ (K. Haggerty & Ericson, 2000). These data doubles may have qualities of the ‘Real’ but they are basically ‘virtual’ based on the simulations in and by computers (Shields, 2003). As personal information through the data doubles becomes readily available over different networks it is easier for people to get hold of the previously private information. An individual can use this information to impersonate an individual, get a credit card, and use the stolen name to run up large bills. According to (“BBC NEWS | UK | When someone else becomes you,” 2003) in 1997, 350,000 cases of identity fraud were reported by a major credit bureau, Trans Union. The propagation of

the idea of global "(in)security" primarily by the U.S. has allowed the U.S. and its allies to enhance surveillance, but only towards certain segments of society.

Biometrics, identity cards, iris scanning are means of surveillance but they have also led to social sorting and discrimination. According to Graham & Wood (2003) people, represented by the personal data that is algorithmically processed to predict future behaviors, are subjected to the effects of discriminatory or inaccurate classification. Richards & King (2014) asserted that individuals are told who they are even before they make their own minds about it. Post 9/11 the American government systematically interrogated over 5000 nationals from the Middle East, only on the basis of their identity. Civil liberties of individuals were ignored as the U.S. centralized and controlled the IT databases containing the personal data of these foreigners or long-term residents. At the European level as well, databases were put in place to permit the profiling of certain individuals. Surveillance of each individual is growing, however, the effective controls and coercive restrictions of freedom are more rigorous towards certain targets. The narrative built by 9/11 has constructed these targets as the 'invisible and powerful enemies in networks' (Bigo, 2006). Surveillance capitalism has centralized power in the hand of few, targeting specific groups, and creating economic, and sociocultural exploitation.

Surveillance capitalism has provided more opportunities to those in power to exploit the general public. The reliance on digital profiling of individuals to predict their preferences has impaired the asymmetry of power between the profilers and the users. This has calamitous connotations for the individuals within the surveilled population. By dividing individuals into small segments through personalized messages, on the basis of their tastes and interest, the strategy of 'divide and conquer' is implemented (Yeung, 2018). Data-driven profiling has also led to personalized pricing for every individual as each customer can just view their own digital shop front. This means that on the basis

of the algorithmic assessment of each shopper's predicted readiness to pay, two individuals can be proffered the same product, at the same time but at separate prices (Townley, Morrison, & Yeung, 2017). It is feared that these practices will create a market divide between a consumer class that receives profligate personal attention, offers and services and a class appraised as 'low value' which is methodically ignored (Yeung, 2018). This divide will further enhance economic injustice in society.

The accumulation of personal data by surveillance capitalists has led to the economic injustice of maldistribution. Data has become an essential corporate asset, an important economic input, and a foundation for new business models. As of yet, the secrecy of the personal data has prevented a thorough analysis of its economic value but inference can be made taking the example of Facebook's initial public offering (IPO). At the time of IPO Facebook's market valuation was $104 billion yet the company claimed assets of just $6.3 billion. The value of its 2.1 trillion pieces of monetizable content was not put by Facebook which is around $100 per user data point (Mayer-Schönberger & Cukier, 2013). This just indicated the worth of one's personal data to the data brokers, not taking into account the future reuse of the data when it is resold to the marketers, creditors, and insurance firms (Cinnamon, 2017). The concentration of wealth in the hands of few companies along with those companies having fewer employees in comparison to the revenue generated has led to economic inequality (Landwehr, Borning, & Wulf, n.d.). This economic inequality is further exploited by organizations as they are not prepared to share the wealth generated by the personal data of individuals with those users themselves (Tene & Polonetsky, 2013). However, the cost of surveillance capitalism is not just the economic injustice of maldistribution but also sociocultural misrecognition, and misrepresentation.

The injustice of misrecognition and misrepresentation due to inaccurate and discriminatory classification is yet another price that is being paid for surveillance capitalism. Our identity and status in the society are now determined by predictive scores determined by surveillance capitalists in the form of credit scores (Wu, 2010), fraud score, ID risk score, churn score (Analytics, 2016), etc. But 25% of credit scores have serious inaccuracies. In most of the other scores, the data and calculation parameters used are impervious, unfettered, and unfamiliar to the public (Dixon & Gellman, 2014). This misrecognition created due to inaccuracy often leads to people not securing a loan, a job, insurance which is unfair (Cinnamon, 2017). This has created a social conflict between those who have our data, and the general public. Moreover, organizations often purposefully develop algorithms to participate in illicit forms of discrimination. Proxy datasets are created, by companies to engage in an unlawful form of discrimination and hide their oppressive behavior (Ohm, 2013). For example, it is illegitimate to discriminate against potential property renters on the basis of their cultural background or socio-demographic features, however, algorithms can be designed that deliberately evade advertising on social media platforms to users that are considered undesirable due to their identity, status, or background (Cinnamon, 2017). Surveillance Capitalism is not just exacerbating social and economic inequality in society, it has repercussions at the individual vlevel as well.

Mass personalization due to surveillance capitalism is nurturing pervasive narcissism. At an individual level surveillance capitalism is fueling everyone's belief in the significance of their preferences, desires, and inclinations. It is catering to the idiosyncratic tastes of individuals (Yeung, 2018). These extreme egotistic tendencies in individuals can create a narcissistic culture that concomitantly leads to social isolation. In the long run, this would undermine a sense of collective, shared identity (Putnam, 2000). This would mark a significant shift from the

community, solidarity towards isolation, and weakening of the principle of equality (Yeung, 2018). The whole notion is not just building a narcissist community, it is also threatening human autonomy and global democratic practices.

Surveillance capitalism is profoundly anti-democratic with data abuses hampering individual autonomy and the basic foundation of democracy, 'free & fair elections'. Surveillance in itself is the polar opposite of democracy when looking from the normative continuum (K. D. Haggerty & Samatas, 2010). Democracy promises freedom to choose while surveillance capitalism endangers human autonomy. The more information is known about an individual, the easier it is to control him/her (Schwartz, 1989). The compromise of individual freedom ultimately leads to totalitarianism. It is a procedure adopted by totalitarian states/capitalists to unjustifiably collect personal data from people for commercial and electoral purposes (Giroux, 2015). Here we can take the example Cambridge Analytica, a data firm that misused the data of 87 million Facebook users without their consent, impeding democracy's basic goal, to conduct free and fair elections. Cambridge Analytica came into limelight in 2018 as it used a Facebook-based quiz app 'thisisyourdigitallife' to collect data from users, shared the data with Donald Trump's election team, and used that information to target US voters with the aid of personalized political messages (Cadwalladr & Graham-Harrison, 2018). This misuse of data compromising democracy was seen in the case of Brazil as well.

Brazil, Russia and many other governments are also employing surveillance technologies for different purposes. Jair Bolsonaro making his way in and becoming the Brazilian President had a lot to do with the misinformation spread through social media. WhatsApp was used by the supporters of Bolsonaro to spread daily misinformation against his competitors in the elections to millions of potential Brazilian voters ("WhatsApp skewed Brazilian election, proving social

media's danger to democracy," 2018). Similarly, a Russian company that has Russian government as one of its customers, downloaded bulk data from Facebook. The leak was not related to demographic information but to the facial recognition models that the Russian authorities might use for surveillance purposes. So all in all, Facebook makes its simpler, easier, attractive for consumers to give their personal information on the platform and then it exploits it and makes it easily accessible to advertisers, governments for misuse (Leetaru, 2018). This again is a fallout of Facebook, its lack of seriousness in tackling privacy concerns and it is now just Facebook, surveillance capitalism and its economic, social, and political implications have now spread to many online companies.

Many online companies, attracted by surveillance capitalism, are misusing data by even making false claims. Snapchat employees used the data of the app to access location data, pictures, and email addresses without the consent of users. Similarly, there are apps that are making false claims saying that they want to help people cope through mental illness or quit smoking. However, in reality, they take user data and sell it to big corporations making those users potential targets for social stigmatization or targeted advertising that aggravates health problems rather than solving them (Johnson, 2019). From misuse of data to injustices, false claims now surveillance capitalists are even posing a threat to national security.

Yet another repercussion of surveillance capitalism is that classified information is becoming public, threatening national security. An open search researcher used data from a fitness app 'Strava' to globally map the U.S military bases. Companies constantly knew what the soldiers were doing as they tracked their runs (Sly, 2018). The Chinese government used social media platforms to profile user behaviors via point-based social credit systems (Landwehr et al., n.d.).

With such severe ramifications of surveillance capitalism, it is important to discuss the general data protection regulation in this age.

The collection, usage, monetization, and capitalism of data traverses' international jurisdictions, the only regulation worth discussing regarding data protection is EU's GDPR law. There are legal challenges associated with data protection (Pagallo, 2017). The most notable law passed to date for restricting data collection and analysis has been the General Data Protection Regulation (EU) which came into effect in 2018. The law gives EU citizens control over their personal data (Andrew & Baker, 2019). The law has placed restrictions on how companies can gather and use personal data, which in turn will hinder the practice of surveillance capitalism. However, there has been a disparity in the implementation of it with 59,000 data breach notifications with just 51 fines imposed since GDPR's inception until January 2019 (Aho & Duffield, 2020). EU's GDPR law is based upon the notion of personal consent, it is a start however amidst the COVID-19 pandemic, surveillance capitalism would just continue to thrive.

COVID-19 pandemic has allowed governments and corporations to continue surveillance capitalism on the pretext of using it to manage distress and control the spread of the virus. There are dangers involved with using technological fixes at a crisis time. Klein (2020) used the term 'Coronavirus Capitalism' being used to pass legislation which would just benefit the privileged and further deepen the inequality. Similarly, an increase in the usage of mental health apps amidst the pandemic will continue to place people as innocent profit-makers. These apps use the vulnerability of individuals at this time and make them part of a clandestine supply chain for the market place without their consent (Cosgrove, Karter, Morrill, & McGinley, 2020).

In Pakistan, there has been no work done by researchers on the phenomenon of Surveillance Capitalism. Even if the factor of capitalism is taken away, just the aspect of surveillance and

monitoring of citizens by its own government and foreign powers has not been explored in detail in the country. Thus, the literature available on surveillance in Pakistan, reports, new pieces, and a couple of research papers have been used to draft the subsequent chapter.

Chapter 2: Surveillance in Pakistan

Surveillance cannot be suppressed as a regional issue, nonetheless, there is variation in its level and intensity from country to country. As populations became increasingly itinerant, relations & transactions stretched elastically into the virtual world, making surveillance increasingly globalized. The events of 11 September 2001 acted as a catalyst to the globalization of surveillance. (Lyon, 2004a). However, surveillance intensity differs regionally. In this chapter, we would try to understand how surveillance has evolved in Pakistan with the rise in information technology, who is conducting surveillance of Pakistanis, what is the law of surveillance, and how surveillance has turned into surveillance capitalism by those in power.

Information Technology and Surveillance in Pakistan

The boom in information technology in Pakistan can be traced back to the 1990s, while in the last decade or so it has completely taken charge of all aspects of our daily lives. It was in the early 1990s that the internet emerged in Pakistan with text-based internet and email communications. Sustainable Development Networking Programme was established in 1992 in Pakistan that helped in boosting computer literacy in the country (Zafar & Ahmad, 2011). Before that in the 70s and early 80s computer import was banned in the country. It was only permitted with the special import license of the Ministry of Commerce (Kundi, 2008). The revolution in information technology, primarily in the last decade has visibly brought about changes in the life of the average people of Pakistan (Rajani & Chandio, 2004). Today, in each and every industry in Pakistan, technology plays a fundamental role, be it financial institutions, educational institutions, automobile industry, civil aviation, telecom, or/and textile market (Abbas et al., 2014). In the banking sector of Pakistan, banks have embraced internet banking as a delivery channel for supplying services (Rahi, Abd.Ghani, & Hafaz Ngah, 2019). Similarly, other sectors have also adopted technological

solutions to daily problems. Today ICT is the fastest growing industry in Pakistan. Here it is also important to discuss the transformation in the mobile telecom industry.

With the adoption of innovative technologies in the country, there has been a continuous expansion in the mobile telecommunication market. From 1990 to 1995, mobile standards and services were introduced in the country. From 1996 to 2003, key institutions and important public policies were formed including the Telecommunications Act 1996 was established to lay the premises for the fast development of the mobile telecommunication industry in the country. Henceforward, licenses were given to new companies. Service providers expanded their networks to serve wider segments of customers (Gao & Rafiq, 2009). With such rapid growth and adoption of ICTs in Pakistan, the tech companies and the government itself began using the technology for surveillance purposes.

Deciphering surveillance in Pakistan requires an understanding of how much data of how many users are accessible to the authorities. The sizeable population of Pakistan generates huge amounts of communications traffic. As of May 2020, Pakistan has 166 million cellular subscribers, 80 million 3G/4G subscribers, 3 million basic telephony subscribers, and 82 million broadband subscribers ("Telecom Indicators | PTA," 2020). Surveillance of all these users by the government is quite comprehensive and tech advanced (*Tipping the Scales: Security & Surveillance in Pakistan*, 2015). Similarly, registration of personal data is pervasive, with SIM cards being registered and biometrically verified through the national database of the National Database and Registration Authority. Having one of the world's most broad citizen registration scheme, almost 96% of Pakistani citizens have biometric ID cards. This also includes the Smart National Identity Card that contains the biometric picture of the owner, a computer chip, address, and names of the parents (NADRA, 2016). This indicates the amount of data available to the authorities, and it does not end here as there is a lot of information is shared on social media platforms as well.

While officially the identity of most Pakistanis exists on the digital database operated by the National Database and Registration Authority (NADRA), most of the people have other digital existences as well. There is a digital existence on social media platforms. There are 37 million social media users in Pakistan as of January 2020, the users increased by 2.4m between April 2019 and January 2020 (Kemp, 2020). Similarly, the digital existence is also formed with the kind of digital services acquired be it online banking, filing tax returns, criminal records, and passports. At airports and other sensitive places, facial recognition software is also used to create digital profiles (Baig, 2019). With extensive data available, surveillance is a reality in Pakistan, however how it became a normal phenomenon in the country would be understood in the subsequent para.

Surveillance in Pakistan by Government & Foreign Powers

Surveillance in Pakistan became an acceptable phenomenon as it was done under the blanket of security and security became a concern, triggered by the September 11, 2001 attack and later expanded due to the 2014 Peshawar school attack by a Taliban-affiliated group. 9/11 compelled countries to take emergency measures for the sake of natural security but at the cost of the rights guaranteed to citizens. Pakistan, being the most active partner of the U.S on the war of terror adopted measures that violated the rights of the citizens (Husain, 2014). They were violated at the pretext of countering insurgent and Islamist groups (*Tipping the Scales: Security & Surveillance in Pakistan*, 2015). Later on, it was the Peshawar massacre that demanded enhancement of surveillance in the country (Muhammad Amir Rana, 2016). Thus, in the name of security, the mass interception of ordinary citizens' communications was carried out. But 'who' was and is carrying it out?

Surveillance of Pakistani citizens is being carried out by the government of Pakistan, intelligence agencies, and even by foreign powers. The government of Pakistan monitors online traffic ("A

Surveillance State," 2019) while intercepted communication is also collected and used by a number of intelligence agencies in Pakistan. Every branch of Pak armed forces has an intelligence service that conducts signals intelligence. Similarly, Inter-Services Intelligence (ISI) and Joint Signal Intelligence Bureau collect data. Different surveillance research projects and development is carried out by the Joint Intelligence Technical and Joint Intelligence X under the Ministry of Science and Technology. Intercepted communication data is also used by the Intelligence Bureau, under the Prime Minister (*Tipping the Scales: Security & Surveillance in Pakistan*, 2015). Foreign powers especially the U.S has also used surveillance against Pak citizens. The Pak government revealed that sensitive data of Pakistan is at risk of being stolen by the U.S (Hussain & Bukhari, 2014). Similarly, Pakistan condemned the US National Security Agency's (NSA) surveillance programme for spying on the PPP back in 2010 (Haider, 2014). Thus, surveillance of Pakistanis is happening both at the national and international levels, with the aid of information technology.

Information technology and surveillance go hand in hand, their combination has an air of inevitability. The relationship between technology and surveillance has been explored by Lyon & Zureik (1996) explaining how new technology has the ability to handle unlimited information and use it for surveillance purposes. Information Communication technologies have no physical boundaries which makes the data users store on it, vulnerable (Imad & Khan, 2019). With the penetration of Information Communication Technologies in Pakistan, the government employed technologies to surveil both people in general and targeted individuals. Surveillance in the country is not just prevalent, some of it is unlawful as well. Only in 2015, ISI tapped 6523 phones in February, 6,819 in March, and 6,742 in April (Malik, 2015). Similarly, the integrated biometric Nadra system allowed the identification of individuals immediately and tracked people in intrusive ways that raised concerns when there were Nadra data breaches (*The Right to Privacy in Pakistan's*

Digital Spaces: April 2018 Human Rights Council Report, 2018). Here it is important to discuss the role of the communication surveillance industry of Pakistan that has led to an increase in the level of surveillance.

The thriving communication surveillance industry of Pakistan has led to an expansion in surveillance activities. There is heavy monitoring of the Voice over Internet Protocol (VoIP) communications which include known services including Skype and Viber. There are limited spaces to communicate privately online. PTA ordered the ban of encryption and virtual private networks (VPNs) to all ISPs and phone companies. Encryptions and VPNs are often used to ensure confidentiality in communications. Their ban barred secure communication of information. Other than PTA companies like the Center for Advanced Research in Engineering and the National Radio Telecommunication Corporation of Pakistan have developed surveillance tools. Similar companies provide the interception technologies and facilities to monitor and analyze transmitted data Foreign companies also provided surveillance centre solution to the Pakistani government. A German surveillance technology company Trovicor and Nokia Siemens Networks (NSN) are two companies worth mentioning. Since the late 1990s, NSN has played a major role in the surveillance market of Pakistan. It was one of the first companies to provide mobile (GSM) network lawful interception capacity in Pakistan (*Tipping the Scales: Security & Surveillance in Pakistan*, 2015). This also indicates that surveillance in Pakistan is not just internally done by the authorities, but also foreign powers are spying on Pakistan.

Surveillance of Pakistan by international organizations and agencies exists. In the case of Pakistan as per Glenn Greenwald (2013) Pakistan is the second-highest most spied country on the list of nations spied on by the United States' National Security Agency (NSA). Also, surveillance of Pakistanis is done by foreign spy agencies as in September 2018, the government issued a warning

to foreign missions and local government officials regarding phone tapings and interception by foreign spy agencies (Haq, 2018). Likewise, in June 2015 it was unveiled that the Pakistan Internet Exchange (PIE) was hacked and insinuated by Britain's GCHQ. This allowed GCHQ to access, store Pakistani users' data (Fishman & Greenwald, 2015). It has been seen how data of Pakistanis users has been exploited by both internal authorities and external powers. Henceforth, it would be discussed whether the surveillance of data occurs with the consent of the Pakistanis government or not.

The surveillance of Pakistanis internally (by its own government) and externally (by foreign powers) occurs most of the time with the consent of the government. The justification given by the government of internal communication surveillance is that the country is in the midst of protracted conflict against armed militant groups within and outside its borders. Surveillance, claimed by the government is essential to counter these threats. A report on ‘’Security & Surveillance” revealed that since at least 2005 mass network surveillance has been in place in Pakistan. The government acquired this technology from both domestic and foreign surveillance companies which include big names Alcatel, Ericsson, Huawei, SS8, and Utimaco (Tipping the Scales: Security & Surveillance in Pakistan, 2015). The report further states that Pakistan’s military and intelligence establishment received heavy funding from the overseas government to build advanced communication surveillance infrastructure. Thus, the surveillance within the country by the government happens with its consent but surveillance is also taking place of Pakistanis by foreign powers.

Global North specifically U.S surveillance of Pakistanis is also taking place most of the time with the consent of the government. Pakistani government and the U.S collaborated in the SKYNET programme of National Security Agency (NSA) in which the caller data was garnered from

Pakistani telecommunications providers. Data was taken from 55 million phone records (*The Right to Privacy in Pakistan's Digital Spaces: April 2018 Human Rights Council Report*, 2018). There were more leaks which pointed out that the entire citizen biometric database of Pakistan was offered to the United States government (*Pakistan government's alleged leaking of citizens' private data is unacceptable - IFEX*, 2017). Be it the CIA and Germany's intelligence service using a Swiss encryption company for spying on Pakistan, India, Iran and other countries (AFP, 2020) or NSA using a powerful data mining tool to gather 13.5 billion intelligence reports from Pakistan in 2013 (W. Desk, 2013), surveillance has been misused time and again. Even though surveillance is often done with the consent of the government, the government has time & again tried to control it as well.

Pakistan, like any other country, has been stuck between two wars, one of fighting against terrorism and the second of protecting the privacy, data, and info of people from being accessed by foreign powers. The digital data of Pakistan is accessed by America, India, and other countries' intelligence agencies. Other than these agencies, the government is also facing cyber-attacks by criminals. Only in Nov 2018, the money of 624 customers at various banks got lost. It amounted to 11.7 million. Similarly, as per a legal report from FIA the data of 19,865 ATM cards of Pakistanis was sold on the dark web. Thus, there is money criminals are making through surveillance and data breaches and then there is also surveillance that is taking place with the consent of the authorities. There has been a price Pakistan has paid for this consensual surveillance of its citizens.

Surveillance Repercussions and Law in Pakistan

Pakistan enjoys access to surveillance technologies with a price to pay. Pakistan is one of the largest recipients of NSA funds. The country receives 'technical solutions and/or access to related

technology' and in exchange, Pakistan provides 'unique access, regional analytical expertise, foreign language capabilities and/or I&W [Intelligence & Warning] support' (Mehmood & Ahmad, 2017). However, this transfer of surveillance technologies is aligned with the security agenda of 'American and European governments, and their allies'. In 2009, cable from the US Embassy in Islamabad discovered by WikiLeaks unveiled that Pakistan in exchange for surveillance technology transfers gave extensive information on its citizens from its National Database and Registration Authority (NADRA, Advanced Passenger Information (API) list, and Passenger Name Records (PNRs) from flights leaving Pakistan to the U.S. The irony of the situation was that the Pakistan government used surveillance technology to keep an eye on its people while the Americans used the info given to them to surveil the government and people respectively (Haider, 2014). Here it is also important to discuss the role played by NADRA in the surveillance of Pakistanis.

The e-surveillance program in Pakistan is linked to the evolution of NADRA. NADRA evolved into a national registry and centralized database of all Pakistani citizens. Under the blanket of security, NADRA sneaked into the lives of the registered citizens. The CNIC number is connected to almost every activity a user does be it banking services, purchasing activity, traveling, SIM card registration (Malkani, 2020). This became evident with the launch of the FBR-NADRA portal, in which personal data of 53m citizens was uploaded online. The data also included the travel history of citizens, which substantiated the lackadaisical attitude of authorities towards the protection of personal data of its citizens (Editorial, 2019). In these citizens, the surveillance of female journalists in Pakistan has been discussed in the literature.

Surveillance of female journalists in Pakistan is being conducted by the state as well as by non-state actors. Female journalists revealed that they were being surveilled for years but due to its

clandestine nature it went undetected. Until they were shown their own private data of years, that they realized that they were being surveilled. Systematic surveillance, they believe is being carried out with the aid of intelligence agencies. It is the technologies that are used as tools to trace the movements of journalists. Thus, the journalists, specifically female journalist have felt and experienced constant surveillance by the government (Digital Rights Foundation, 2017). Even though here a specific segment of society has been discussed that has faced surveillance, it is happening to every citizens. This has reduced citizens to data points, giving up their basic right to privacy.

The discernible fallout of surveillance is the erosion of the privacy of the people. Surveillance done to restrict privacy can only be justified if it is essential for achieving a legitimate goal, and is proportionate to the goal pursued (*International Principles on the Application of Human Rights to Communications Surveillance*, 2013). However, it is suspected that intelligence agencies conduct wire-tapping and various forms of modem surveillance without any rules, guidelines, or restrictions by the judiciary for decades (Husain, 2014). Similarly, with reports like sale of 115 million Pakistanis mobile phone data online on the dark web (Zakir, 2020), news of government acquiring services of a controversial Canada-based company 'Sandvine' to monitor all incoming and outgoing internet traffic in the country (M. Desk, 2019), the excuses given for privacy misuse are hard to digest. With this it is essential to look at the legality of this by studying the constitution of Pakistan regarding privacy.

The constitution of Pakistan does have a right to privacy, but it is vague in terms of information privacy. In Pakistan's Constitution under Article 14(1) the right to privacy is stated in these words, "[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable" (Aziz, Senior, Associate, Noor, & Research, 2020). Similarly, under Article 10A the right to a fair trial is

guaranteed which poises the right to privacy with the duty of the state to investigate criminal matters (Hafeezullah Ishaq, 2014). However, there is no foundation laid down by courts in Pakistan regarding the right of one's Information Privacy. Thus, presently the citizens of Pakistan cannot prevent information privacy as there are no statutory rules to control the use or sharing of their private information. There are no cybercrime laws in Pakistan currently (Yameen, 2014). There is a need for a new data protection law in Pakistan to allow the citizens of the country to have more control over their personal data (Daudpota, 2016). Recently, Pakistan has introduced a draft of the data protection bill, however, even that bill does not have clauses regarding the protection of data against the government and state surveillance (Khilji, 2019). It is also essential that Pakistan collaborates with other countries like India to have harmonized cyberlaws. In case of India and Pakistan (Yameen, 2014) said it is important that both the countries find ways of building trust in the information space. He suggested that both the countries can collaborate on having a joint law on cybercrime. It is important to have effective laws against surveillance, which deal at it at national and international levels.

As digital technology bypass the bindings of national boundaries, the law for surveillance must have a well thought of mechanism for international cooperation. Companies that collect, and store user data are often not even registered locally, thus the local law can not be enforced on them. It is vital to have data protection and privacy law that protects the privacy of Pakistanis at both national and international level. General Data Protection Regulation (GDPR) is an example of how a law is made to protect the privacy of citizens across the EU (Baig, 2019). Baig (2019) further stated that with increased state surveillance it is also essential to enhance awareness amongst the legal and judicial groups. There have been instances where FIA investigative officers were not concerned about the privacy invasion that happens if an individual's digital devices are analyzed

without following appropriate legal procedures. The public also needs to be aware of how their digital identities kept by Facebook, Google, and national corporations are stored, saved, and distributed (Baig, 2019). With an effective privacy law in Pakistan, the situation might improve, however it seems that surveillance would continue to thrive in the world hit by COVID-19 pandemic.

From 9/11 to the APS attack, surveillance has been vindicated for security reasons in Pakistan, and today COVID-19 is the justification given for mass surveillance. ISI is in command of tracing and tracking individuals who have been in contact with people who tested positive for the virus. It is a matter of concern that an increase in state surveillance will further legitimize the infringement of privacy rights, information, data protection, and freedom (Jahangir, 2020). While it is understandable that surveillance is being done to control the coronavirus cases, privacy breaches can be avoided by using anonymized data. It would ensure that instead of personal information unique identifiers are used for collecting data. Similarly, the government needs to be transparent about any data-sharing agreements with the public and private sector entities. Moreover, data needs to be encrypted so that recipients can share the data without misusing it (RSIL, 2020). Here another concern is that even when COVID-19 ends, is there any procedure in place to ensure that the surveillance initiated because of the pandemic is put to an end, or will it be continued to serve purposes not related to coronavirus (Ahmed, 2020). Up until now the aspect of surveillance in Pakistan has been discussed, henceforth it will be discussed why surveillance is being conducted in the country and what is it leading to.

Understanding the purpose behind surveillance in Pakistan and worldwide is key to grasping its repercussions on human beings as individuals and societies at large. Hitherto, it has been studied how surveillance has been carried out within Pakistan and internationally. Besides this, it was

discussed how surveillance is a direct attack on one's privacy. The law of privacy in Pakistan was explained in detail.

In the ensuing chapter the phenomena not discussed by researchers in Pakistan yet, that is of 'Surveillance Capitalism' will be explored in detail. In earlier times surveillance was executed to win wars, but in the age of technology, 'data' is the new currency and the path of acquiring that data comes through surveillance. Thus, surveillance is done to gain capital, earn money, and be superior. This is what Zuboff (2019) termed as 'The Age of Surveillance Capitalism'. Surveillance Capitalism commodifies personal data for profit-making. The surveillant capitalists benefitting from surveillance capitalism have created a divide between those in the power of data, and the public. This is leading to inequalities in society.

Globally, those benefitting from Surveillance capitalism are in the following order; tech companies at the top and then the government, advertising firms, and telecom sector subsequently. A handful of giant technology companies (Facebook, Google, Microsoft, Apple, Amazon) possess and control our information. They, work as surveillance intermediaries, having the power to share it or not share it with the ad companies, and the government respectively (Rozenshtein et al., 2018). Apple won the legal battle with the FBI in 2016 as it withheld information from the government regarding giving them access to an iPhone used by a terrorist. So even the government surveillance has its dependence on technology companies that seem to hold the supreme power in this regard (Arash Khamooshi, 2016). In Pakistan, big data and AI analytics used for data generation primarily benefit private telecom companies, multinationals, and local banks (Haq, 2016). This in turn can lead to economic inequalities in society.

The global economic power rests with the big tech be it the Big 5 companies of the United States or the rising tech giants of China i.e. Tencent and Alibaba (Fallon, 2018), their dominance has

exacerbated a shift in income from labor to capital. This has led to economic inequality globally. It will be discussed how it is leading to economic inequality in Pakistan in Chapter 3.

Similarly, Surveillance Capitalism has amplified the existing social inequalities, reproducing regimes of control leading to the exclusion of marginalized groups in societies. Cinnamon (2017), Wu (2010) have in detail explained how our identity is determined by predictive scores developed by surveillance capitalists, but inaccuracies in it can lead to misrecognition. Also, Ohm (2013) explains how often discrimination against certain groups using surveillance is often purposeful and illegal. In Pakistan, the apathetic consequence of Surveillance Capitalism in Pakistan is seen in case of inequality towards Pashtun through their ethnic and racial profiling, as claimed by the Pashtun Tahafuz Movement (PTM) (Khan, 2019). In just the twin cities of Pakistan, 5400 Pashtun from FATA were placed under strict surveillance as the government deliberated 'issuing them chip-based national identity cards equipped with security features'. Surveillance of this sort aided in mass killings of Pashtun, and a similar level of surveillance, and harassment have also been faced by the Balochi community (Rabia Mehmood & Mavish Ahmad, 2017). Furthermore, how surveillance capitalism is creating a social divide in society will be studied in Chapter 3.

Economic control, social inequality allows surveillance capitalists to produce a regime for the abstract control of populations. Homeless shelters give in to the agencies/capitalists collecting data of the homeless to have access to federal funds as these homeless people submit to the usage of their experiences into abstract "universal data elements" in exchange for survival (Willse, 2015). The surveillance system for the care of elderly does no just diagnose and understand behavioral patterns but also use surveillance system to 'control' and 'manage' elderly people, depicting their power (Kenner, 2008). This economic and social inequality by Surveillance Capitalists is giving

them absolute control. In Pakistan, how these inequalities can/can not lead to the conflict would be discussed in the subsequent chapter.

Who comes to powers in the U.S, Pakistan or any other democratic state should be the decision of the general public, but with surveillance capitalists in play, it is they who decide. Elections are engineered in the U.S, revealed an expert from the U.S. In the Cambridge Analytica case, the whole campaign was targeted towards the voters who were confused about whom to vote to. Are they also engineered in Pakistan or not? This question would also be answered in the next chapter.

The next chapter would explore the phenomenon of surveillance capitalism in Pakistan. Also, various themes catering to inequalities, conflict, and legal aspects of surveillance capitalism will be discussed.

Chapter 3: Surveillance Capitalism in Pakistan, Analysis, and Discussion

This chapter presents an analysis of the responses given by the 9 respondents interviewed for this respective study. The respondents were an expert from the U.S, a Cryptography Professor at the Institute of Space Technology (IST), a Technical Analyst at Elixir Technologies, a Former PTA representative, a current PTA data analyst, a bank worker, a cybersecurity specialist, a NADRA official, and the Director Research and Policy Digital Rights Foundation. Broadly speaking there are two categories of respondents. Four of them belonged to government organizations. They were interviewed to get a real insight into whether the government organizations indulge in surveillance activities or not, while five are surveillance experts, and they knew how surveillance capitalism is taking place in Pakistan. 7 out of the 9 respondents wished to remain anonymous, thus their names will not be mentioned in the analysis. While two of the respondents, 'Shmyla Khan' Director Research and Policy Digital Rights Foundation, and 'Dr. Amin' the cryptography professor permitted using their name in the present study.

This research was conducted to explore how the phenomenon of surveillance capitalism is taking place in Pakistan. The themes that will be discussed in this chapter are 'Surveillance Capitalism and Discrepancy in Responses', 'Role of 9/11', 'Surveillance Capitalism & Advertising Firms', 'Surveillance Capitalism & Economic Inequality', 'Surveillance Capitalism and Social Inequality', 'Risk of Conflict', and 'Privacy law in Pakistan with respect to Surveillance Capitalism'.

Surveillance is a phenomenon globally present. Even if surveillance was considered as a domain of nation-state or of firms within a nation-state, it has changed in the 21st century. Now surveillance has rapidly become globalized (Lyon, 2004). In Pakistan its existence is undeniable as discussed in Chapter 2; however, a discrepancy was visible in accepting the existence of surveillance

amongst the respondents of this research. Four respondents belonged to government organizations. Three of these four respondents completely denied the existence of surveillance. One of the respondents, a representative from the state-owned enterprise Pakistan Telecommunication Authority (PTA) was asked about the surveillance carried out by the organization, the representative denied that any form of surveillance is used by the organization. There was hesitancy by the worker in answering most of the questions. Similarly, when a former PTA employee was approached with similar queries, the respondent wanted to tone down the word 'surveillance' with 'monitoring' stating that in general surveillance has a negative connotation. The respondent stated that PTA does not interfere in the private usage of IT services. Another respondent a bank employee revealed that "Bank has great policies. All the information is stored in the head office and it stays there." This unacceptance of surveillance is discussed in the literature in terms of socially desirable and undesirable topics. Respondents tend to have discomfort while answering a sensitive question (Krumpal, 2013). However, one of the government workers, a NADRA official accepted that surveillance is a reality present in Pakistan.

The industry experts were more candid in their responses. Cyber industry specialists, digital rights expert, and the cryptography professor were more vocal in accepting the existence of surveillance in the country. The cryptography professor, taking a neutral approach stated that Information technology can be used to gather both legitimate and illegitimate information as the process is the same. One of the respondents divulged that surveillance stands at 65% in Pakistan. Further stating that in the U.S it is much higher. In Pakistan, due to a lack of infrastructure and a centralized system, full surveillance output cannot be obtained. It is understandable that while government workers have their confidentialities, cyber analysts, or/and the cryptography professor do not have such reservations, thus they can be more candid in their responses.

Most of the respondents started off the discussion about surveillance in Pakistan by giving a reference to 9/11. Since September 11, 2001, more extensive security strategies were employed with intensive surveillance and control to prevent future such incidents (Levi & Wall, 2004). Thus, surveillance cannot be talked about in isolation to the 9/11 incident. All of the respondents excluding the ones that belonged to a government organization stated that 9/11 paved that path for the use of mass surveillance in the country. One of the respondents brought this to light that after 9/11 all dollar transactions in Pakistan went through the U.S, even if they were minimal amount transactions. So the economic activity of Pakistan was under watch/surveillance as the U.S believed that it is through the economic activity that terrorism was increasing. One of the respondents said that 9/11 increased our tolerance for surveillance as it was done under the pretext of security. From 9/11 till up till now there was no question asked from the government about the surveillance of citizens. As most of the respondents agreed that 9/11 was an incident that enhanced surveillance activities in the country, it was now important to address as to how data from surveillance was used for monetization and capitalism in the country.

To find out whether surveillance is generating capital for those in power in the country, the respondents of the research were inquired about how data can be used for multiple purposes. The current and former PTA representatives identified the positive sides of how data can be used for improving services for users. The PTA representative stated that data can be used to improve user experience, improve services. Another respondent said that today every department/ organization in the public domain is making its data available on its website as long as it is not confidential and against the interests of the country. Such data is used to enhance commercial activity. Due to the WEB, individuals and businesses are able to publish their services and products at competitive

prices and make it available to the remotest parts of the world (Former PTA employee, 2020). The rest of the respondents highlighted how data is being misused in the country.

While it is true that data can and is being used to improve customer services, it is being exploited as well, as highlighted by some of the respondents of the present study. The NADRA official accepted that data is being misused by companies, though the official revealed that there are many Pakistanis that are not even registered to NADRA, which does restrict surveillance via the organization's database. Similarly, the cryptography professor, building on a similar narrative said that data is being exploited. Nobody asks you for your consent that your data is being used or kept by international organizations. Adding to it, the professor also unveiled that the U.S has a complete database containing names of the people they have doubt about related to terrorism and if they get a transaction of a similar name, they hold that transaction. This highlighted the extent of our data available to the international authorities.

Another theme that emerged from the responses of most of the respondents was 'Surveillance Capitalism and Advertising Firms'. Advertising firms collect and trade users' data for behavioral advertising (Pal & Crowcroft, 2019). The respondents other than the PTA officials agreed on this view that data is bought by companies without user consent so that they can make predictions about users to ultimately generate capital. The cybersecurity specialist was of the view that advertising has been happening for ages. Companies have tried to make ads to target audience aiming to generate capital. However now by misusing data to manipulate audiences into buying products is a breach of user privacy, thus it is an issue. Similarly, the Director Research and Policy Digital Rights Foundation Shmyla Khan (2020) stated that it is openly known that the data leaked for instance from NADRA records are sold to anyone in general, but usually, they are marketing/ad companies, the cybersecurity specialist also in similar words revealed that there have been data

leaks that revealed how data is being sold by the Big 5 companies. The expert from the U.S gave more details of how ‘Codes’ are attached to every user on the internet, these codes have complete info about the user. That data is later purchased usually by advertising companies to be used for capitalism and monetization. Similarly, one of the respondents said that even in the television programmes viewed by the viewers, the ad companies know which programme is being watched, how much, and which ad should be placed accordingly through our data. Another respondent disclosed that every activity on every app used by users be it WhatsApp, Maps, GPS, is monitored. This data is collected and then sold to AliExpress, amazon, mobile companies, digital advertisement companies, web crawlers. This highlighted that there are a handful of companies, primarily ad companies that have hold of user data and they are generating capital from it.

‘Economic Inequality’, was a point that was highlighted by various respondents in different ways. When the respondents were asked about the economic worth of data of Pakistanis to certain organizations/governments. The respondents gave varied responses to it. The former PTA representative stated that assuming the question is related to public data, the worth varies from subject to subject. For economic development, all positive data should be presented to attract attention and we should be fair to the utmost when providing details. The cryptography professor Amin (2020), and the cybersecurity specialist had similar responses of how the U.S has all our data, Amin said that they have a record of all the dollar transactions while the cybersecurity specialist said that all the data on NADRA is kept by the U.S authorities and U.S embassies, which in turn gives them the power to access our info and earn money. On the contrary, when a NADRA official was approached with this question, the official said that if data is asked by officials for official purposes, then it is given, otherwise, NADRA is extremely secure. Elaborating on it the

official said that the data from NADRA can not be hacked or misused. Thus, unless the organization shares the information for official purposes by itself, user data remain secure.

This in itself indicates that those in power have access to all our data, widening the divide between the general public and those in power. This divide is not just between the government and the people, it is largely between the leading tech giants and the rest of the world.

The economic divide between tech companies and the public was highlighted by the respondents. The expert from the U.S responded that due to surveillance capitalism money is in the hand of just a few companies. It is the tech companies that are earning, they have the economic power, which in turn is increasing the divide between those in power, and the public. On similar lines, Shmyla Khan (2020) said that the big tech companies, the kind of profit they are making, even during a pandemic when there is economic recession all over the world, Jeff Bezos became a trillionaire, Zoom recording record profit, these companies are thriving, they have been able to do it because there is lack of regulation. Another respondent, the technical analyst Javad (2020) said surveillance early on was done to win wars, today it is done to gain capital, be superior which in turn is leading to the economic divide in the society. So while most of the respondents agreed that surveillance capitalism is leading to economic inequality in the society, they were divided on ‘how’.

One of the major themes that were discussed by almost every respondent was of how surveillance capitalism is leading to social inequality in society. Surveillance allows the state to sort individuals by either including or excluding them, influencing their chances in life (Monahan, 2008) . While the former PTA representative said that the question is not relevant to telecom and the current PTA representative stated that data is used to start projects in rural areas that benefit the society at large, both of them avoided the aspect of ‘inequality’ from the equation. The rest of the respondents were vocal in their responses. They said that the profile of every individual is made, they are judged,

misrecognized, and misrepresented based on those profiles which lead to social inequality in the society. One of the respondents stated about how societal inequality is done through social engineering, systematic bullying, and campaigning, so his response catered to the societal inequality created through surveillance capitalism. An interesting aspect was discussed by one of the respondents stating that technology is written by human beings who have certain biases, prejudices and their biases are replicated in society as they have the power to do so. When Amazon was using a recruiting tool to screen CVs, no women were chosen by that algorithm, as the algorithm was based on the existing workforce which was already male-dominated. This is a clear example of how surveillance capitalism leads to social inequality.

The literature of this study also highlighted how surveillance was used as a tool to hamper U.S elections. So, the questions also touched on the aspect of whether in Pakistan, surveillance capitalism is used for election hampering. Most of the respondents' response to this was this can not be said for sure. While the expert from the U.S said that in the Cambridge Analytica case, the campaign was targeted against people who were confused, not sure whom to vote to. This must be happening in Pakistan as well, though not as effectively as in the U.S. Now election teams would have youngsters who understand the technology and how it operates in your favor. Similarly, one of the respondents' Director Research and Policy Digital Rights Foundation Shmyla (2020) stated that in terms of political maneuvering (Cambridge Analytica) type situation there is very little that can be speculated. However, it a known fact that political parties used targeted ads like sending SMS to people in a constituency. For instance, PTI even had a constituency app to rally people on election day. Now connecting this to surveillance or a party to know which person is likely to vote for them, the data of such type might exist and might be used as well but we can’t say for sure as the Election Commission does not ask for that kind of transparency. So we can just speculate, but

without having any evidence it can not be said for sure. However, this is something to be worked upon, as the next elections come, this approach can be weaponized/used to maneuver elections similar to what happened in the U.S, or/and Brazil. The NADRA official informed that the election campaigning that takes place in the U.S can not be compared with Pakistan. This is because many of the citizens are not even biometrically registered. There are many that have genuine issues like sweating in their hands, thus they can not be registered. In such a situation using data of Pakistanis to hamper elections is not practically possible right now. With a lot of discussion on surveillance capitalism, its repercussions, the discussion with the respondents shifted towards the legal aspect of the phenomena.

Respondents were asked about why is there no check-in Pakistan, what is the legal aspect of surveillance capitalism. While the former PTA representative again repeated that the question, isn't relevant to telecom, a couple of respondents explained in detail the law of Pakistan regarding privacy. The cryptography professor said that there is an almost negligible constitutional or legal check against organizations misusing user data. It is important to build such institutions that define that personal data of users will not be exploited for multi-purposes The cyber specialist went ahead and said that Pakistan does not have any law for privacy. Even the rules made for cybersecurity were made invalid a few years ago. Similarly, Shmyla (2020) highlighted a point regarding the law of privacy stating that even if legislation is passed, there is a lot of power that the government has in terms of making exceptions within that law so that it can exempt certain government departments. Thus, it would be useless in terms of government surveillance or the data that the government collects of its people. This response indicated that even laws made by those in power are constructed in a way that they make sure they remain in power, continue surveillance, continue to gain money at the expense of public data.

One of the most important aspects discussed with the respondents was of surveillance capitalism and its repercussion on the conflict in the future in the country. This question not just prompted a variety of answers, but also each respondent had a different perspective. While a respondent said that every country may be having its own tech apps and working in isolation in the future, another respondent said that we have not reached the level of conflict yet. All we can do is take consent of people, do not misuse their self-respect. Another respondent said that he can see a conflict in the future created through social engineering. Interestingly, a respondent linked to conflict with power and control, saying that when security agencies will know that the user data is sold to individuals as well, they would put more restrictions, while all the control would remain with them. In another way, another respondent gave a similar response stating that even if initiatives are taken similar to the rise in Green technology or technology being used for counter-surveillance to amplify voices of marginalized people, the model of technology is so embedded in the capitalist structure that perpetuates all kind of inequalities, that it is difficult to get out of it. Even if these companies try to help people or take initiatives for the protection of the privacy of people, they are not able to let go of the power, which can in turn lead to conflict in a society. While reviewing the responses of the respondents there were some noteworthy deductions made by the researcher which will be discussed in the second half of the chapter.

Surveillance capitalism in Pakistan, its existence was denied by the PTA representatives interviewed in this research. This denial by those in power can be a concerning factor as most of the other respondents not just acknowledged the existence of surveillance capitalism but also explained how it is and it can further lead to economic, and social inequality in Pakistan. The disparate control structures of contemporary institutions catalyzed by surveillance shape the experiences and life chances of different people, differently. This divide is a problem, which needs

addressing. If the government does not acknowledge and address this problem, it can have not just anticipated but also unanticipated repercussions.

Thus, it is of utmost importance that we as a society concede it so that necessary steps can be taken to bring about policies and data protection laws in the country like EU's GDPR law.

Also, while interviewing respondents for this study, some in denial, some being neutral, some accepting, and informing how surveillance capitalism is an issue in the country, the researcher observed that a balance is lacking. A balance of using surveillance for the right purposes, to control terrorism, and keeping user privacy intact. The tech companies and the government should not conduct surveillance activities unless it is absolutely necessary for security purposes. Misuse of user data by authorities does not just raise ethical concerns, it has far-reaching consequences. Someone out there is using our data and making money, without our consent or our knowledge. Someone out there is judging us through the data they have about us. Someone out there is manipulating us into making decisions we might not have made otherwise. We are being automated. This problem is global, but the solution has to be made by every nation for itself. The data protection law for Pakistan has to be drafted by its government, for its citizens.

Conclusion

Surveillance, 'overseeing', 'watching' and 'monitoring' others have encroached and whittled away privacy. But surveillance capitalism is not just erosion of individual space. Monetization of surveillance centers around the logic of data commoditization. Data is commoditized by surveillance capitalists who in turn enable an asymmetric redistribution of power. The power & economic balance, shift towards the actors, that have access to our information, which in turn has magnified economic inequality in the society. Similarly, surveillance capitalists use digital data to profile individuals. Profiling is never fully accurate. Inaccuracy in profiling can stigmatize citizens as criminals or poor credit risks (Gilbert, 2007). This is yet another repercussion of surveillance capitalism, leading to social injustice in society. The most significant impact of surveillance capitalism was seen in the case of Cambridge Analytica, in which data of 87 million Facebook users was misused without their consent, hampering the basic notion of democracy, conducting free and fair elections.

The theoretical framework of Deleuze and Guattari is used in this study to understand surveillance. Deleuze has explained how we are inhabiting in control societies where corporations have a single objective, that is to have complete command over individuals through ceaseless surveillance. Building on this theoretical framework of control societies, Shoshana Zuboff's conceptual framework of 'Surveillance Capitalism' is used in this research to explore the phenomenon in Pakistan.

The first chapter explored the literature on Surveillance Capitalism. In the literature, the theoretical framework, conceptual framework, and empirical findings on surveillance capitalism are discussed. The second chapter touched on the aspect of Surveillance in Pakistan. In this chapter, it is discussed as to how surveillance is being carried out within Pakistan by authorities and how

foreign powers are also conducting surveillance on Pakistan, many times with their consent. The repercussions of this phenomenon and the law of Pakistan regarding privacy are explained in detail. In the third and last chapter, the study was conducted by the researcher to find the existence of surveillance capitalism in the country and discuss its repercussions with the respondents in the shape of economic and social inequalities and risk of conflict.

Inequalities, be it economic or social, have existed in the world incessantly. Surveillance capitalists are widening that gap. Technology, in itself, is merely a tool, it is the surveillance capitalists with their biases and thirst for power and capital, who are exploiting that technology.

In Pakistan, the first and foremost thing is for authorities to be transparent about surveillance activities. As long as it is being done to protect citizens, to control terrorism it is essential. However, when capitalists try to capitalize on surveillance, it is problematic. It can and is leading to an economic and social divide in the country. Its repercussions are far-reaching as those that have our data can control and are controlling us in ways we can't fathom. This, surveillance capitalism is and will continue to bring about economic inequality, social conflict in society.

While concluding this paper, it must be stressed that even though the present study looked at the phenomenon of surveillance capitalism in Pakistan, it is a global issue. For the last two decades, surveillance capitalists were able to bypass laws and regulations, in the name of security. They know all about us, while we know nothing about them, further widening the social inequality by creating inequality in the division of learning.

The paper has its limitations, especially keeping this in view that it is written at a time when the world is hit by the COVID-19 pandemic. Trying to reach out to people for interviews was difficult considering the situation at hand. Also, the nature of the study was such that many potential

respondents backed out upon hearing the gist of the study. This makes it even more important to talk about Surveillance Capitalism.

There is a conflict that is brewing through the inequalities generated by surveillance capitalism under the blanket of peace and security. It is high time, that not just Pakistan, the world gets a grip on the situation. The EU data protection law with GDPR is just a start. We need similar data protection laws in Pakistan and worldwide. Here it is essential that academics, cyber experts, digital right experts, and even government officials start talking and writing about it. This paper in itself is a small effort to bring this issue to the limelight, create a healthy discussion on the topic to bring a constructive change before it gets too late.

References

A Surveillance State. (2019). Retrieved July 12, 2020, from https://nation.com.pk/26-Oct-2019/a-surveillance-state

Aas, K. F., Gundhus, H. O., & Lomell, H. M. (2009). *Technologies of inSecurity : the surveillance of everyday life*. Routledge-Cavendish.

Abbas, J., Muzaffar, A., Mahmood, H. K., Ramzan, M. A., Sibt, S., & Rizvi, U. H. (2014). Impact of Technology on Performance of Employees (A Case Study on Allied Bank Ltd, Pakistan). *World Applied Sciences Journal*, *29*(2), 271–276. https://doi.org/10.5829/idosi.wasj.2014.29.02.1897

AFP. (2020). CIA spied on Pakistan, other countries through Swiss encryption firm: report. Retrieved May 14, 2020, from https://www.thenews.com.pk/print/613221-cia-spied-on-pakistan-other-countries-through-swiss-encryption-firm-report

Ahmed, R. (2020). Track and trace | Pakistan Today. *PakistanToday*. Retrieved from https://www.pakistantoday.com.pk/2020/06/01/track-and-trace/

Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, *49*(2), 187–212. https://doi.org/10.1080/03085147.2019.1690275

Allen, M. (2019). What is Hyperscale and How is it Shaping the IT Industry? Retrieved February 10, 2020, from Data Centers website:

https://www.datacenters.com/news/what-is-hyperscale-and-how-is-it-shaping-the-it-industry

Analytics, V. (2016). Predictive Scores: Deriving meaningful intelligence from complex assortments of data. Retrieved February 17, 2020, from https://versium.com/tech-glossary-term/predictive-analytics

Andrew, J., & Baker, M. (2019). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-019-04239-z

Arash Khamooshi. (2016). Breaking Down Apple's iPhone Fight With the U.S. Government - The New York Times. Retrieved May 15, 2020, from https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html

Atta, Q., & Haq, U. (2019). Computer Network and Information Security. *Computer Network and Information Security*, *1*, 62–69. https://doi.org/10.5815/ijcnis.2019.01.06

Attride-Stirling, J. (2001). Thematic networks: An analytic tool for qualitative research. *Qualitative Research*, *1*(3), 385–405. https://doi.org/10.1177/146879410100100307

Aziz, J., Senior, A. M., Associate, R., Noor, R., & Research, F. (2020). *The COVID-19 Law & Policy Challenge: Public Health vs. Individual Privacy in the Age of Cyber Surveillance*.

Baig, A. (2019). *Privacy in the digital age | Special Report | thenews.com.pk*. Retrieved from https://www.thenews.com.pk/tns/detail/568763-privacy-digital-age

Bailey, J. (2008). First steps in qualitative data analysis: Transcribing. *Family Practice*, *25*(2), 127–131. https://doi.org/10.1093/fampra/cmn003

Barr, A. (2015). How Google Aims to Delve Deeper Into Users' Lives - WSJ. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/how-google-aims-to-delve-deeper-into-users-lives-1432856623

Bauman, Z. (1998). *Globalization : the human consequences*. Columbia University Press.

BBC NEWS | UK | When someone else becomes you. (2003). Retrieved January 13, 2020, from http://news.bbc.co.uk/2/hi/uk_news/2800767.stm

Bergen, M., & Kantrowitz, A. (2014, May 21). Verizon Looks to Target Its Mobile Subscribers With Ads | Ad Age. *Advertising Age*. Retrieved from https://adage.com/article/digital/verizon-target-mobile-subscribers-ads/293356

Bigo, D. (2006). Security, exception, ban and surveillance. *Theorizing Surveillance: The Panopticon and Beyond*.

Bogard, W. (2006). *Surveillance assemblages and lines of flight*. 111–136. https://doi.org/10.4324/9781843926818-11

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brunon-Ernst, A. (2016). *Deconstructing Panopticism into the Plural Panopticons*. 33–58. https://doi.org/10.4324/9781315569192-8

Bryman, A. (2001). *Social Research Methods by Alan Bryman*. Retrieved from https://www.amazon.com/Social-Research-Methods-Bryman-2001-05-10/dp/B01FEP5SZC

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach | News | The Guardian. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606. https://doi.org/10.1207/s15506878jobem4604_6

Carr, E. C. J., & Worth, A. (2001). The use of the telephone interview for research. *NT Research*, *6*(1), 511–524. https://doi.org/10.1177/136140960100600107

Castells, M., Castells, & Manuel. (2004). *Informationalism, networks, and the network society: a theoretical blueprint*.

Cinnamon, J. (2017). Social injustice in surveillance capitalism. *Surveillance and Society*, *15*(5), 609–625. https://doi.org/10.24908/ss.v15i5.6433

Cohen, J. E. (2016). The regulatory state in the information age. *Theoretical Inquiries in Law*, *17*(2), 369–414. https://doi.org/10.1515/til-2016-0015

Cosgrove, L., Karter, J. M., Morrill, Z., & McGinley, M. (2020). Psychology and Surveillance Capitalism: The Risk of Pushing Mental Health Apps During the COVID-19 Pandemic. *Journal of Humanistic Psychology*, *60*(5), 611–625. https://doi.org/10.1177/0022167820937498

Creswell, J. (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches: Creswell, John W.: 8601404516801: Amazon.com: Books*. Retrieved from https://www.amazon.com/Qualitative-Inquiry-Research-Design-Approaches/dp/1412995302

Daudpota, F. (2016). … Pakistan's Courts have not been able to lay down any scope for the right of one's Information Privacy (which involves the establishment of rules governing collection and handling of personal data such as credit information and medical records) …. *SSRN Electronic Journal*. Retrieved from https://ssrn.com/abstract=2866416

Deleuze, G. (1992). *Postscript on the Societies of Control* (Vol. 59). Retrieved from http://www.jstor.org/about/terms.html.

Deleuze, G., & Guattari, F. (1987). *A THOUSAND PLATEAUS Capitalism and Schizophrenia*. Retrieved from http://www.upress.umn.edu

Desk, M. (2019). Govt working with controversial firm to monitor internet traffic: report - Newspaper - DAWN.COM. Retrieved May 15, 2020, from https://www.dawn.com/news/1512784

Desk, W. (2013). US agency collected second-highest amount of digital data from Pakistan | The Express Tribune. Retrieved May 14, 2020, from https://tribune.com.pk/story/560949/us-agency-collected-second-highest-amount-of-digital-data-from-pakistan/

Digital Rights Foundation. (2017). *Surveillance of Female Journalists in Pakistan*. Retrieved from https://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Surveillance-of-Female-Journalists-in-Pakistan-1.pdf

Dixon, P., & Gellman, R. (2014). *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future Brief Summary of Report About the World Privacy Forum*. Retrieved from www.worldprivacyforum.org.

Editorial. (2019). FBR-Nadra portal - Newspaper - DAWN.COM. *DAWN*. Retrieved from https://www.dawn.com/news/1490305

Edwards, D. (2011). *I'm feeling lucky : the confessions of Google employee number 59*. Houghton Mifflin Harcourt.

Facebook muscles its way to 71% earnings surge | Financial Times. (2017). Retrieved February 9, 2020, from https://www.ft.com/content/e99ee0ce-723a-11e7-aca6-c6bd07df1a3c

Fallon, I. (2018). Global economic power rests with big tech - The National. Retrieved May 15, 2020, from https://www.thenational.ae/business/technology/global-economic-power-rests-with-big-tech-1.700274

Faulhaber, G. R. (2011). Economics of net neutrality: A review. *Communications & Convergence Review*, *3*(1), 53–64. https://doi.org/10.0000/PAPERS.SSRN.COM/1894286

Fishman, A., & Greenwald, G. (2015). *Spies Hacked Computers Thanks to Sweeping Secret Warrants, Aggressively Stretching U.K. Law*. Retrieved from https://theintercept.com/2015/06/22/gchq-reverse-engineering-warrants/

Flick, U. (2018). *The SAGE Handbook of Qualitative Data Collection - Google Books*. Retrieved from https://books.google.com.pk/books?hl=en&lr=&id=X0VBDwAAQBAJ&oi=fnd&pg=PP1&dq=the+sage+handbook+of+qualitative+data+collection+pdf&ots=AVce8y2Bs5&sig=HDcrYqf5JPjYLE4_go1VFsvLGp4#v=onepage&q=the sage handbook of qualitative data collection pdf&f=false

Foucault, M. (1979). *Discipline & Punishment: the Birth of the Prison*. Retrieved from http://en.wikipedia.org/wiki/Discipline_and_Punish

Galič, M., Timan, T., & Koops, B. J. (2017). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy and Technology*, *30*(1), 9–37. https://doi.org/10.1007/s13347-016-0219-1

Gallagher, R. (2014). *The Surveillance Engine: How the NSA Built Its Own Secret Google*. Retrieved from https://firstlook.org/theintercept/article/2014/08/25/icreach-nsa-cia-secre...

Gandhewar, N., & Sheikh, R. (2009). Google Android: An Emerging Software Platform For Mobile Devices. In *Article in International Journal of Advanced Trends in Computer Science and Engineering*. Retrieved from https://www.researchgate.net/publication/266371721

Gandy, O. H., & Herbert Schiller Professor, J. I. (2002). *Data mining and surveillance in the post-9.11 environment*.

Gao, P., & Rafiq, A. (2009). The transformation of the mobile telecommunications industry in Pakistan: A developing country perspective. *Telecommunications Policy*, *33*(5–6), 309–323. https://doi.org/10.1016/j.telpol.2009.03.001

Gates, K. A. (2011). Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance on JSTOR. *NYU Press*. Retrieved from https://www.jstor.org/stable/j.ctt9qg8xd

Gilbert, N. (2007). Dilemmas of privacy and surveillance: Challenges of technological change. *Criminal Justice Matters*, *68*(1), 41–42. https://doi.org/10.1080/09627250708553288

Giroux, H. A. (2015). Totalitarian Paranoia in the Post-Orwellian Surveillance State. *Cultural Studies*, *29*(2), 108–140. https://doi.org/10.1080/09502386.2014.917118

Given, L. (2012). The SAGE Encyclopedia of Qualitative Research Methods. In *The SAGE Encyclopedia of Qualitative Research Methods*. https://doi.org/10.4135/9781412963909

Glenn Greenwald. (2013). Boundless Informant: the NSA's secret tool to track global surveillance data | NSA | The Guardian. Retrieved May 12, 2020, from https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining?CMP=twt_gu#_

Graham, S., & Wood, D. (2003). Digitizing Surveillance: Categorization, Space, Inequality. *Critical Social Policy*, *23*(2), 227–248. https://doi.org/10.1177/0261018303023002006

Gregory, D. (2011). The everywhere war. *The Geographical Journal*, *177*(3), 238–250. https://doi.org/10.1111/j.1475-4959.2011.00426.x

Groom, V., & Calo, R. (2011). *Reversing the Privacy Paradox: An Experimental Study*.

Gubrium, J. F., Holstein, J. A., Marvasti, A. B., & McKinney, K. D. (2012). The SAGE handbook of interview research: The complexity of the craft, second edition. In *The SAGE Handbook of Interview Research: The Complexity of the Craft*. https://doi.org/10.4135/9781452218403

Hafeezullah Ishaq, H. (2014). *The Right to Fair Trial: Better Late than Never*. Retrieved from http://unyearbook.un.org/unyearbook.html?name=194849index.html

Haggerty, K. D., & Samatas, M. (2010). *Surveillance and democracy*. Routledge.

Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Haider, M. (2014). *Pakistan lodges formal protest with US against PPP surveillance - Pakistan - DAWN.COM*. Retrieved from https://www.dawn.com/news/1116802

Haider, M. (2014). PPP slams US spying, says violators owe an apology - Pakistan - DAWN.COM. Retrieved May 15, 2020, from https://www.dawn.com/news/1116565/ppp-slams-us-spying-says-violators-owe-an-apology

Haq, R. (2018). Govt issues phone tapping alert | The Express Tribune. Retrieved July 12, 2020, from https://tribune.com.pk/story/1814567/hostile-agencies-intercepting-official-communication-authorities-warned

Haq, S. (2016). Tech expert dives into big data potential in Pakistan | The Express Tribune. Retrieved May 15, 2020, from https://tribune.com.pk/story/1151447/telecommunication-tech-expert-dives-big-data-potential-pakistan/

Hardt, M., & Negri, A. (2000). *Empire*. Harvard University Press.

Hawkins, J. E. (2018). The Practical Utility and Suitability of Email Interviews in Qualitative Research Repository Citation. *Nursing Faculty Publications*. Retrieved from https://digitalcommons.odu.edu/nursing_fac_pubs

Hoffmann, A. L., Proferes, N., & Zimmer, M. (2018). "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media and Society*, *20*(1), 199–218. https://doi.org/10.1177/1461444816660784

Hoofnagle, C. J. (2009). Beyond Google and evil: How policy makers, journalists and consumers should talk differently about Google and privacy. *First Monday*, *14*(4). https://doi.org/10.5210/fm.v14i4.2326

Husain, W. (2014). *SURVEILLANCE AND LAW ENFORCEMENT: TOOLS IN THE FIGHT AGAINST TERROR IN A COMPARATIVE STUDY OF THE UNITED STATES AND PAKISTAN*. Retrieved from http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf

Hussain, F., & Bukhari, G. (2014). *Pakistan | Global Information Society Watch*. Retrieved from https://www.giswatch.org/en/country-report/communications-surveillance/pakistan#_ftn7

Imad, M., & Khan, A. (2019). CYBER-WARFARE: IMPLICATIONS FOR THE NATIONAL SECURITY OF PAKISTAN. In *NDU Journal*.

International Principles on the Application of Human Rights to Communications Surveillance. (2013).

Jahangir, S. (2020). *Is surveillance during COVID-19 subtly legitimising the state's control in Pakistan? | Special Report | thenews.com.pk*. Retrieved from https://www.thenews.com.pk/tns/detail/652610-states-writ-peoples-rights

Jeffries, A. (2017, November 15). Why is this company tracking where you are on Thanksgiving? | The Outline. *The Outline*. Retrieved from https://theoutline.com/post/2490/why-is-this-company-tracking-where-you-are-on-thanksgiving?zd=1&zi=346ivio6

Johnson, C. (2019). *Big Tech Surveillance Could Damage Democracy*. Retrieved from https://scholarworks.boisestate.edu/uar_2019/8

Kemp, S. (2020). *Digital 2020: Pakistan — DataReportal – Global Digital Insights*. Retrieved from https://datareportal.com/reports/digital-2020-pakistan

Kenner, A. M. (2008). Securing the elderly body: Dementia, surveillance, and the politics of “aging in place.” *Surveillance and Society*, *5*(3), 252–269. https://doi.org/10.24908/ss.v5i3.3423

Khan, S. (2019). Battling Orwellian surveillance in Pakistan | Special Report | thenews.com.pk. *The News*. Retrieved from https://www.thenews.com.pk/tns/detail/589543-battling-orwellian-surveillance

Khan, S. (2019). Social Sorting as a Tool for Surveillance | Heinrich Böll Stiftung | Brussels office - European Union. Retrieved May 15, 2020, from https://eu.boell.org/en/2019/01/21/social-sorting-tool-surveillance

Khilji, U. (2019). *Data protection law - Newspaper - DAWN.COM*. Retrieved from https://www.dawn.com/news/1455963

Kirkpatrick, D. (2010). *The Facebook effect : the inside story of the company that is connecting the world*. Simon & Schuster.

Klein, N. (2020). Coronavirus Capitalism — and How to Beat It. *The Intercept*. Retrieved from https://theintercept.com/2020/03/16/coronavirus-capitalism/

Krumpal, I. (2013, June 19). Determinants of social desirability bias in sensitive surveys: A literature review. *Quality and Quantity*, Vol. 47, pp. 2025–2047. https://doi.org/10.1007/s11135-011-9640-9

Kundi, G. M. (2008). DIGITAL PAKISTAN: OPPORTUNITIES & CHALLENGES. *JISTEM Journal of Information Systems and Technology Management*, *5*(2), 365–390. https://doi.org/10.4301/s1807-17752008000200009

Landwehr, M., Borning, A., & Wulf, V. (2019). The High Cost of Free Services. *Proceedings of the Fifth Workshop on Computing within Limits - LIMITS '19*, 1–10. https://doi.org/10.1145/3338103.3338106

Landwehr, M., Borning, A., & Wulf, V. (n.d.). *The High Cost of Free Services: Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure*. https://doi.org/10.1145/3338103.3338106

Leetaru, K. (2018). What Facebook's Russian Data Leak Shows About Government Surveillance And Facial Recognition. *Forbes*. Retrieved from https://www.forbes.com/sites/kalevleetaru/2018/10/13/what-facebooks-russian-data-leak-shows-about-government-surveillance-and-facial-recognition/#1b6d24891045

Lehtiniemi, T. (2017). Personal data spaces: An intervention in surveillance capitalism? *Surveillance and Society*, *15*(5), 629–639. https://doi.org/10.24908/ss.v15i5.6424

Levi, M., & Wall, D. S. (2004, June). Technologies, security, and privacy in the post-9/11 European information society. *Journal of Law and Society*, Vol. 31, pp. 194–220. https://doi.org/10.1111/j.1467-6478.2004.00287.x

Levy, S. (2011). *In the plex : how Google thinks, works, and shapes our lives*. Simon & Schuster.

Lyon, D. (2003). *Surveillance after September 11*. Polity Press in association with Blackwell Pub. Inc.

Lyon, D. (2003). Technology vs "terrorism": Circuits of city surveillance since September 11th. *International Journal of Urban and Regional Research*, *27*(3), 666–678. https://doi.org/10.1111/1468-2427.00473

Lyon, D. (2004). Globalizing Surveillance. *International Sociology*, *19*(2), 135–149. https://doi.org/10.1177/0268580904042897

Lyon, D. (2004). Globalizing Surveillance: Comparative and Sociological Perspectives. *International Sociology*, *19*(2), 135–149. https://doi.org/10.1177/0268580904042897

Lyon, D. (2004). Surveillance Technology and Surveillance Society. In *Modernity and Technology*.

Lyon, D. (2006). Theorizing surveillance: The panopticon and beyond. In *Theorizing Surveillance: The Panopticon and Beyond*. https://doi.org/10.4324/9781843926818

Lyon, D. (2010). Surveillance, Power and Everyday Life. In *Emerging Digital Spaces in Contemporary Society* (pp. 107–120). https://doi.org/10.1057/9780230299047_18

Lyon, D., & Haggerty, K. D. (2012). The Surveillance Legacies of 9/11: Recalling, Reflecting on, and Rethinking Surveillance in the Security Era. *Canadian Journal of Law and Society, 27*(3), 291–300. https://doi.org/10.1017/S0829320100010516

Lyon, D., & Zureik, E. (1996). *Computers, surveillance, and privacy*. University of Minnesota Press.

Malik, H. (2015). *Phone-tapping: SC to take up ISI's plea for in-camera hearing on Wednesday | The Express Tribune*. Retrieved from https://tribune.com.pk/story/904267/phone-tapping-sc-to-take-up-isis-plea-for-in-camera-hearing-on-wednesday

Malkani, A. (2020). *Pakistan: Without data protection & privacy laws, Internet can be misused*. Retrieved from https://www.asianage.com/opinion/oped/020320/pakistan-without-data-protection-privacy-laws-internet-can-be-misused.html

Manokha, I. (n.d.). *Surveillance: The DNA of Platform Capital-The Case of Cambridge Analytica Put into Perspective*.

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance and Society, 1*(1), 9–29. https://doi.org/10.24908/ss.v1i1.3391

Maxwell, J. (2013). *Qualitative Research Design: An Interactive Approach*. Retrieved from

https://books.google.com.pk/books/about/Qualitative_Research_Design_An_Intera cti.html?id=DFZc28cayiUC&redir_esc=y

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data : a revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mayo, R. C., & Leung, J. (2018, May 1). Artificial intelligence and deep learning – Radiology's next frontier? *Clinical Imaging*, Vol. 49, pp. 87–88. https://doi.org/10.1016/j.clinimag.2017.11.007

McCahill, M. (2002). *The Surveillance Web : the Rise of Visual Surveillance in an English City*. Willan Pub.

McLaughlin, K., & Sullivan, M. (2017). Google's Relentless AI Appetite — The Information. *The Information*. Retrieved from https://www.theinformation.com/articles/googles-relentless-ai-appetite

Mehmood, R., & Ahmad, M. (2017). Surveillance, Authoritarianism and 'Imperial Effects' in Pakistan. *Surveillance & Society*. https://doi.org/10.24908/SS.V15I3/4.6721

Miller, A. R. (1969). Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society. *Michigan Law Review*, *67*(6), 1089. https://doi.org/10.2307/1287516

Misa, T. J., Brey, P., & Feenberg, A. (2003). *Modernity and technology*. MIT Press.

Monahan, T. (2008). *Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance*. Retrieved from https://ssrn.com/abstract=3035028

Muhammad Amir Rana. (2016). *After Peshawar: Reassessing the terror threat - DAWN.COM*. Retrieved from https://www.dawn.com/news/1151616

Munhall, P. L. (1989). Philosophical ponderings on qualitative research methods in nursing. *Nursing Science Quarterly*, *2*(1), 20–28. https://doi.org/10.1177/089431848900200109

NADRA Pakistan – National Database & Registration Authority Official Website. (n.d.). Retrieved July 12, 2020, from https://www.nadra.gov.pk/

NADRA. (2016). Smart-Computerized-National-Identity-Card – NADRA Pakistan. Retrieved July 12, 2020, from https://www.nadra.gov.pk/smart-computerized-national-identity-card/

Neal, D., & Rahman, S. M. (2012). Video surveillance in the cloud-computing? *2012 7th International Conference on Electrical and Computer Engineering, ICECE 2012*, 58–61. https://doi.org/10.1109/ICECE.2012.6471484

Nock, S. L. (1993). *The costs of privacy : surveillance and reputation in America*. A. De Gruyter.

Norris, C., & Armstrong, G. (1999). *The Maximum Surveillance Society: The Rise of CCTV*.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1), 160940691773384. https://doi.org/10.1177/1609406917733847

Ohm, P. (2013). Changing the rules: General principles for data use and analysis. In *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 96–111). https://doi.org/10.1017/CBO9781107590205.006

Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in qualitative research. *Journal of Nursing Scholarship*, *33*(1), 93–96. https://doi.org/10.1111/j.1547-5069.2001.00093.x

Pagallo, U. (2017). The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection. *European Data Protection Law Review (EDPL)*, *3*. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/edpl3&id=42&div=&collection=

Pakistan government's alleged leaking of citizens' private data is unacceptable - IFEX. (2017). Retrieved from https://ifex.org/pakistan-governments-alleged-leaking-of-citizens-private-data-is-unacceptable/

Pal, R., & Crowcroft, J. (2019, July 1). Privacy trading in the surveillance capitalism age viewpoints on "privacy-preserving" societal value creation. *Computer Communication Review*, Vol. 49, pp. 26–31. https://doi.org/10.1145/3371927.3371931

Pasquale, F. (2013). *PRIVACY, ANTITRUST, AND POWER*. Retrieved from http://www.microsoft.com/us/download/details.aspx?id=35596.

Penney, J. W., Nash, V., Gasser, U., Wright, J., Deibert, R., Mathias, J. N., … Bambauer, D. (2015). Chilling Effects: Online Surveillance and Wikipedia Use Recommended Citation CHILLING EFFECTS: ONLINE SURVEILLANCE AND WIKIPEDIA USE. *Berkeley Technology Law Journal*, *31*, 1. https://doi.org/10.15779/Z38SS13

Putnam, R. D. (2000). Bowling Alone: America's Declining Social Capital. In *Culture and Politics* (pp. 223–234). https://doi.org/10.1007/978-1-349-62965-7_12

Radin, M. J. (2014). *Boilerplate : the fine print, vanishing rights, and the rule of law*. Princeton Univ Press.

Rahi, S., Abd.Ghani, M., & Hafaz Ngah, A. (2019). Integration of unified theory of acceptance and use of technology in internet banking adoption setting: Evidence from Pakistan. *Technology in Society*, *58*, 101120. https://doi.org/10.1016/j.techsoc.2019.03.003

Rajani, M. K., & Chandio, M. S. (2004). Use of Internet and its effects on our Society. In *National Conference on Emerging Technologies*.

Richards, N. M., & King, J. (2014, May 19). *Big Data Ethics*.

Robins, L. N. (1963). The Reluctant Respondent. *The Public Opinion Quarterly*, *27*, 276–286. https://doi.org/10.2307/2746922

Roosendaal, A. (2012). Facebook Tracks and Traces Everyone: Like This! *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1717563

Rozenshtein, A. Z., Bamzai, A., Clopton, Z., Daskal, J., Davidson, S., Deeks, A., … Wittes, B. (2018). *Surveillance Intermediaries*.

RSIL. (2020). *Health v. Privacy in the Age of Cyber Surveillance* . Retrieved from https://rsilpak.org/2020/health-v-privacy-in-the-age-of-cyber-surveillance/

Schwartz, P. (1989). The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. *The American Journal of Comparative Law*, *37*(4), 675. https://doi.org/10.2307/840221

Shields, R. (2003). *The virtual*. Routledge.

Sinha, G. A. (2014). *SINHA-FINAL (DO NOT DELETE) NSA SURVEILLANCE SINCE 9/11 AND THE HUMAN RIGHT TO PRIVACY*. Retrieved from http://www.the

Sly, L. (2018, January). U.S. soldiers are revealing sensitive and dangerous information by jogging - The Washington Post. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

Solove, D. (2008). *Understanding Privacy*. Retrieved from https://ssrn.com/abstract=1127888

Staples, W. G. (1997). *The culture of surveillance : discipline and social control in the United States*. St. Martin's Press.

Swedberg, R. (2018). *On the Uses of Exploratory Research and Exploratory Studies in Social Science*. Retrieved from http://people.soc.cornell.edu/swedberg/On the Uses of Exploratory Research and Exploratory Studies in Social Science.pdf

Swire, P. (1999). *Financial Privacy and the Theory of High-Tech Government Surveillance* (Vol. 77). Retrieved from http://www.osu.edu/units/law/swire.htm

Swire, P. (2013). *The Second Wave of Global Privacy Protection: Symposium Introduction*. Retrieved from www.oecd.org/sti/ieconomy/44945

Telecom Indicators | PTA. (2020). Retrieved July 12, 2020, from https://www.pta.gov.pk/en/telecom-indicators

Tene, O., & Polonetsky, J. (2013). Issue 5 Article 1 2013 Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. In *Northwestern Journal of Technology and Intellectual Property* (Vol. 11). Retrieved from https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

THE CONSTITUTION OF THE ISLAMIC REPUBLIC OF PAKISTAN NATIONAL ASSEMBLY OF PAKISTAN. (2012).

The Right to Privacy in Pakistan's Digital Spaces: April 2018 Human Rights Council Report. (2018). Retrieved from www.freedomhouse.org/report/freedom-net/2016/pakistan

Thomas, S., & Pollio, H. (2002). *Listening to Patients: A Phenomenological Approach to Nursing Research and ... - Sandra P. Thomas, Howard R. Pollio - Google Books*. Retrieved from https://books.google.com.pk/books/about/Listening_to_Patients.html?id=qnz1xPKS_38C&redir_esc=y

Thorne, S. (2000, July 1). Data analysis in qualitative research. *Evidence-Based Nursing*, Vol. 3, pp. 68–70. https://doi.org/10.1136/ebn.3.3.68

Tipping the Scales: Security & Surveillance in Pakistan. (2015). Retrieved from https://privacyinternational.org/sites/default/files/2018-08/PAKISTAN REPORT HIGH RES 20150721_0.pdf

Townley, C., Morrison, E., & Yeung, K. (2017). Big Data and Personalized Price Discrimination in EU Competition Law. *Yearbook of European Law*, *36*, 683–748. https://doi.org/10.1093/YEL/YEX015

US4063229A - Article surveillance - Google Patents. (n.d.). Retrieved April 12, 2020, from https://patents.google.com/patent/US4063229A/en

Van Der Ploeg, I. (2005). *Biometric Identification Technologies : Ethical Implications of the Informatization of the Body*. Retrieved from http://www.biteproject.org/.

WhatsApp skewed Brazilian election, proving social media's danger to democracy. (2018). *The Conversation*. Retrieved from https://theconversation.com/whatsapp-skewed-brazilian-election-proving-social-medias-danger-to-democracy-106476

When Big Data Marketing Becomes Stalking - Scientific American. (n.d.). Retrieved January 14, 2020, from https://www.scientificamerican.com/article/when-big-data-marketing-becomes-stalking/

Whitson, J., & Haggerty, K. (2008). Identity theft and the care of the virtual self. *Economy and Society*, *37*(4), 572–594. https://doi.org/10.1080/03085140802357950

Willse, C. (2015). *The value of homelessness : managing surplus life in the United States*.

Wu, C. C. (2010). *Automated Injustice: How a Mechanized Dispute System Frustrates Consumers Seeking to Fix Errors in Their Credit Reports, 14 N.C. Banking Inst*. Retrieved from http://scholarship.law.unc.edu/ncbi/vol14/iss1/6

Yameen, T. (2014). *Cyberspace CBMs between Pakistan and India*. Retrieved from http://www.nust.edu.pk/NP/Publication/Pages/Cyberspace-CBMs-between-Pakistan-and-India.aspx

Yeung, K. (2018). Five Fears About Mass Predictive Personalisation in an Age of Surveillance Capitalism. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3266800

Zafar, F., & Ahmad, S. (2011). *The challenge of internet rights in Pakistan | Global Information Society Watch*. Retrieved from https://www.giswatch.org/en/country-report/internet-rights/challenge-internet-rights-pakistan

Zakir, H. (2020). 115 Million Pakistani Mobile Users Data Go on Sale on Dark Web, claims cybersec company. Retrieved May 15, 2020, from https://www.techjuice.pk/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web/

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, *28*(1), 10–29. https://doi.org/10.1177/1095796018819461

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for Freedom and Power in the Age of Surveillance Capitalism*. Public Affairs, U.S.