Social Media User Surveillance as a Cyber Security Threat: A Case Study of Pakistan

By

Zunairah Qureshi

(Registration No: 00000401255)

Department of Peace and Conflict Studies

Centre of International Peace and Stability

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2024)

Social Media User Surveillance as a Cyber Security Threat:

A Case Study of Pakistan

By

Zunairah Qureshi

(Registration No: 00000401255)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Master of Strategic Studies

Supervisor: Dr. Rubina Waseem

Centre of International Peace and Stability

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2024)

THESIS ACCEPTANCE CERTIFICATE

Certified that the final copy of MS Thesis titled **"Social Media User Surveillance as a Cyber Security Threat: A Case Study of Pakistan"** written by **Ms. Zunairah Qureshi** (Registration No. 00000401255), of **Center of International Peace and Stability** has been vetted by the undersigned, found complete in all respects as per NUST Statutes/ Regulations/ Masters Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for the award of Masters degree. It is further certified that necessary amendments as pointed out by GEC members and evaluators of the scholar have also been incorporated in the said thesis.

Signature: ______________

Name of Supervisor: Dr. Rubina Waseem

Date: 16/08/2024

Signature (HOD): ______________

HoD PCS
Centre for International Peace and Stability
NUST Institute of Peace and Conflict Studies
Islamabad

Date: 16/08/2024

Signature (Dean/ Principal): ______________

ASSOCIATE DEAN
Centre for International Peace and Stability
NUST Institute of Peace and conflict Studies
Islamabad

FORM TH-4
(MUST BE TYPE WRITTEN)

National University of Sciences & Technology

MASTER THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by:

(Student Name & Regn No.)____Zunairah Qureshi 401255____

Titled: Social Media User Surveillance as a Cyber Security Threat: A Case Study of Pakistan be accepted in partial fulfillment of the requirements for the award of __ MS Strategic Studies degree and awarded grade ____._____(Initial).

Examination Committee Members

1. Name: Dr Ansar Jamil Signature:________

2. Name: Dr Tughral Yamin Signature: Tughral Yamin

3. Name:________ Signature:________

Supervisor's name: Dr. Rubina Waseem Signature:________

Date:________

____
Head of Department
HoD PCS
Centre for International Peace and Stability
NUST Institute of Peace and C

____
Date

COUNTERSINGED

Date:________

ASSOCIATE DEAN
Centre for International Peace and Stability
UST Institute of Peace and conflict Studies
Islamabad

____
Dean/Principal

CERTIFICATE OF APPROVAL

This is to certify that the research work presented in this thesis, entitled "**Social Media User Surveillance as a Cyber Security Threat: A Case Study of Pakistan**" was conducted by Ms. **Zunairah Qureshi** under the supervision of **Dr. Rubina Wasim** No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the **Center of International Peace and Stability** in partial fulfillment of the requirements for the degree of Master of Science in Field of **Strategic Studies** Department of Peace and Conflict Studies National University of Sciences and Technology, Islamabad.

Student Name: Zunairah Qureshi Signature: ____________

Examination Committee:

a) External Examiner 1: Name Ansar Jamil

Signature: ____________

Head of Department, Strategic Studies, CIPS, NUST, H-12 Campus, Islamabad

b) External Examiner 2: Name Dr. Tughral Yamin

Signature: Tughral Yamin

Name of Supervisor: Dr. Rubina Waseem

Signature: ____________

Name of Dean/HOD: Dr. Ansar Jamil

Signature: ____________

HoD PCS
...national Peace and Stability
NUST Institute of Peace and Conflict Studies
Islamabad

AUTHOR'S DECLARATION

I, Zunairah Qureshi hereby state that my MS thesis titled "Social Media User Surveillance as a Cyber Security Threat: A Case Study of Pakistan " is my own work and has not been submitted previously by me for taking any degree from National University of Sciences and Technology, Islamabad or anywhere else in the country/ world.

At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Name of Student: Zunairah Qureshi

Date: 08/08/2024

PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis **"Social Media User Surveillance as a Cyber Security Threat: A Case Study of Pakistan"** is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and National University of Sciences and Technology (NUST), Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the University reserves the rights to withdraw/revoke my MS degree and that HEC and NUST, Islamabad have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized thesis.

Student Signature:——————

Name: Zunairah Qureshi

Date: 16/08/2024

DEDICATION

Dedicated to myself for surviving this stars-misaligning tumble down a road paved with scorn and gorgeous blooms—and to my ammi, for surviving me.

ACKNOWLEDGEMENTS

This thesis is but one part of a larger journey; a twisty, tumultuous turn in my life that grated me much but, begrudgingly, also taught me much. A good part of it, I remained whining and floundering about trying to figure the point of any of this, but, in my heart, I knew all along. So, here's a huge, greater-than-the-size-of-Jupiter thank you to my parents for driving me (literally) along this path and supporting me throughout. To my nana, nani, for their endless duas. To Dr Rubina, for believing in my half-cooked ideas and reading through this document multiple times. Similarly, to Dr Tughral—who is one of the coolest people I have had the pleasure of meeting, and whose course was, hands down, the best one I took during my degree—for inspiring this thesis and always encouraging me. To Mahnoor, without whom my time at NUST would have been positively and absolutely unbearable. A huge thank you to all my dear friends for being the strength that I greatly rely on. To Anisa, Amnah, Badam, Maham, Mashal, Neha, for their invaluable proofreading services—and especially to Mari, for too many things to possibly list down. To Tuz and Fati, for their emotional support and counselling services. To my brother, for being my chauffeur and ally. And finally, to my little sister, without whom I wouldn't be able to tell the difference between blue and aquamarine, between elation and happiness, or between love and being loved.

Also, of course to Allah for giving me something I didn't even know I needed.

Contents

List of Tables

List of Figures

LIST OF SYMBOLS, ABBREVIATIONS ANDACRONYMS

BJP Bharatiya Janata Party
CERT Cyber Emergency Response Team
DRF Digital Right’s Foundation
EEA European Economic Areas
EU European Union
FISA Foreign Intelligence Surveillance Act
GDPR General Data Protection Regulation
HUMINT Human intelligence
IoT Internet of Things
NADRA National Database and Registration Authority
PECA Pakistan Electronic Crimes Act
PII Personally Identifiable Information
PTA Pakistan Telecommunication Authority
SOCMINT Social Media Intelligence
TECHINT Technical Intelligence
UGC User-Generated Content
VR Virtual Reality

Abstract

User data privacy is an issue that has only become more concerning in the age of data economy and surveillance capitalism. Major social media companies—this research focuses on Facebook and YouTube—reign supreme with access to unlimited user data. However, data is also acquired through extensive forms of surveillance that go beyond profiling individuals based on their social media activity to tracking their other online as well as offline activity. The data collected then is also made accessible to third-party agents as well as state agencies. This is precisely why the issue of social media user surveillance becomes a cybersecurity threat to citizens' data which, this research argues, is a collective asset integral to national security. Countries such as China, and the EU recognise this as they enforce laws against social media companies. Pakistan, however, with its lack of awareness regarding data privacy at the policy and consumer level, severely lags behind. This research aims to frame the issue of social media user surveillance and data collection as a cybersecurity threat for Pakistan, and thereby affirm that existing policy is not effective against it. For this purpose, it applies realism as its theoretical framework which aptly explains data sovereignty—a concept that is at the core of this study's hypothesis. The research primarily employs qualitative research methods by conducting a comparative critical analysis of selected social media companies' policies and Pakistan's cybersecurity policies and legal framework. The findings of the analysis prove essential in determining the gaps in existing policy and what issues an effective regulatory social media data policy must address.

Keywords: Social media surveillance, data privacy, data sovereignty, big data, Pakistan's cyber security

Chapter 1

INTRODUCTION

The aim of the study is to analyse the growth of social media and its ever-evolving technological advancement which has transformed the world as we used to know it. In this age, social media lends itself to a space that constitutes a digital reality populated by the human existences of its 4.77 billion users worldwide.[1] While this has revolutionised many aspects of life such as allowing easy access to information and faster communication, it has also birthed new challenges. Social media's conversion of people's personal details and private information into data commodities at an unprecedented scale is an emerging challenge from a security point of view. And this has only become a greater cause of concern in the age of data economy and surveillance capitalism, wherein businesses glean profit from user data acquired through various forms of consensual and non-consensual surveillance. Users not only commit their personal identification details when registering on a social media platform, but also continue to give pieces of vital information by simply engaging with the apps on a day-to-day basis. It is no secret that the data collected by social media companies is further sold or made accessible to third-party agents which include advertisers, service providers, and state agencies, among others. This then brings into question how such activity compromises users' data privacy and exposes citizens' data—which is to be understood as a collective national asset—at a scale that makes user surveillance a cyber security threat at the national level. So far, Pakistan's understanding of cyber security is limited to the protection of basic cyber infrastructure and checking criminal activities that are conducted via online mediums.

There is scarcity of literature that addresses data privacy or regulation of social media's data surveillance practices. Given that in 2023, the number of social media users in

[1] Simon Kemp. *Digital 2023: Global Overview Report.* Singapore: DataReportal, 2023. https://datareportal.com/reports/digital-2023-global-overview-report

Pakistan has increased to 72.9 million,[2] social media regulation and understanding of its security is an imperative. Other nations, such as China and the European Union (EU), have made attempts to implement data regulation policies.[3] The EU's General Data Protection Regulation (GDPR) is widely recognised as the most prominent framework for data regulation policy. Recently, Pakistan took the initiative to pass the Data Protection and the e-safety bills which at the very least, attempt to engage with the question of citizens' data on social media. However, as this research will go on to highlight, these policies have been met with serious criticism and appear to severely lack especially in terms of their practicality.

This research will primarily explore the question of how lack of effective social media regulation policies threatens Pakistan's cyber security. It will do so by employing the concept of surveillance capitalism as its conceptual framework and qualitative research methods. The social media companies that this research will cover are Facebook and YouTube, the two most used social media platforms in Pakistan.[4] The research methods will comprise a critical analysis of the social media companies' privacy policies. This will be accompanied by a review of Pakistan's existing cyber security policies which will be compared to the findings from the privacy policies' analysis to identify gaps in local policies.

1.1 Literature Review

A literature review of relevant topic areas helps inform the direction and scope of a study by elucidating important information, research that has already been undertaken, and the approaches that have been applied. In this way, a comprehensive

[2] OOSGA. *Social Media in Pakistan – 2023 Stats and Platform Trends.* Singapore: OOSGA, 2023. https://oosga.com/social-media/pak/

[3] Qin, Bei, David Strömberg, and Yanhui Wu. "Why does China allow freer social media? Protests versus surveillance and propaganda." *Journal of Economic Perspectives* 31, no. 1 (February 2017): 117-140. https://pubs.aeaweb.org/doi/pdf/10.1257/jep.31.1.117

[4] Pakistan Telecommunication Authority. *Annual Report 2023*. https://www.pta.gov.pk/assets/media/pta_annual_report_12022024.pdf.

review summarises the salient points of past and ongoing research. It also reveals literature gaps which can be addressed through further research.

This literature review focuses on research done in the areas of social media surveillance and cybersecurity, both on a general level as well as within the particular context of Pakistan. Prominent themes covered by the review include, the emerging challenges of surveillance capitalism and big data, social media cyber threats, current landscape of cyber security in Pakistan, and social media intelligence. The review also highlights literature gaps that help situate the purpose and course of this research, especially as it pertains to the specific context of Pakistan.

1.1.1 The Emerging Challenge of Surveillance Capitalism and Big Data

Harvard professor and social psychologist, Shoshana Zuboff conceptualised the economic model of surveillance capitalism and outlined its impact on global socio-economic conditions. Surveillance capitalism is the newest rendition of market capitalism wherein the personal data of people is 'mined' on a large scale, most prominently through social media and the wider digital space. This data mining or extraction can often take the form of invasive privacy violations.[5] Under the order of surveillance capitalism and what is also known as the "data economy", humans become a literal resource site, and their actions, behaviours, thoughts, and identities, all become commodifiable data, which is the raw material in this scenario.[6] The scale at which data is now generated and processed has rightly coined the term big data. A lot of research has been done on the subject of big data, which has vastly contributed to improving quality of life through its use in various areas,[7] such as social development, urban design, healthcare, online

[5] Shoshana Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* (London: Profile Books, 2019).

[6] Zuboff. *Age of surveillance capitalism*.

[7] Dylan Maltby. "Big data analytics." Paper presented at *74th Annual Meeting of the Association for Information Science and Technology (ASIST)*, New Orleans, N.O., USA, October 7 – 12, 2011. https://shorturl.at/otcOX.

services, and others. However, at the same time, the challenges that big data poses to privacy and security are questions still grappled with.[8]

Other problems include the inaccuracy of big data in representing real-world contexts and complexities, which has resulted in datasets inheriting cultural biases and homogenisation of diverse identities that cannot be reduced to quantitative data alone.[9] Structural inequalities also exist because only a few nations dominate the big data market. This means only some countries, such as the US, China, Israel, and Russia have the technology to impose surveillance mechanisms[10] on other countries that do not have the knowledge base or infrastructure to either compete with them or protect themselves. From a national security perspective, this becomes a serious concern as it is a well-known fact that state agencies have access to the vast stores of big data that is collected by companies from a global user base.[11] Fusch and Trottier explain how social media enables state surveillance by allowing state and private companies access to its store of data.[12] The Snowden leaks revealed that government agencies, specifically the American, British, and Canadian ones, were commonly engaged in monitoring large populations. Their methods of surveillance included accessing data collected through corporations, public institutions, and of course the internet, where social media platforms proved to be the most fruit-bearing.[13] Since then, as we will further explore in this research, surveillance technologies have only become more advanced and penetrative with increased application of artificial intelligence and the growth of the data industry in general.

[8] Maltby. "Big data analytics."

[9] Xerxes Minocher and Caelyn Randall, “Predictable Policing: New Technology, Old Bias, and Future Resistance in Big Data Surveillance,” *Convergence* 26, no. 5–6 (December 2020): 1108–24, https://doi.org/10.1177/1354856520933838.

[10] Zuboff. *Age of surveillance capitalism*.

[11] Zuboff.

[12] Fuchs, Christian, and Daniel Trottier. "Towards a theoretical model of social media surveillance in contemporary society." *Communications* 40, no. 1 (March 2015): 113-135. https://westminsterresearch.westminster.ac.uk/download/c8923c6f244eb5a1fe92376cdee5cf6b967af4df315fc17109bc872bc94aeaf0/3293718/surv.pdf

[13] David Lyon, “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique,” *Big Data and Society* 1, no. 2 (July 2014): 1–13, https://doi.org/10.1177/2053951714541861.

Given the rate of technological advancement, it is a truly difficult task to keep up with the ever-evolving, emerging challenges of surveillance capitalism and big data. In terms of state security, the most hardline approach has been taken by China, which does not allow foreign social media and other websites to operate within its borders.[14] Instead, it has encouraged the widespread use of local applications that allow it to retain control of its own citizens' data, which it then utilises to implement mechanisms such as social reward systems and predictive policing.[15] The EU, on the other hand, has prioritised its citizens' right to privacy through the GDPR, which mandates websites to be more transparent about the information they collect behind the scenes and allow users options to opt-out.[16] However, while the EU is still working on a policy that is solely dedicated to regulating social media platforms, even the GDPR has been critiqued for lacking practicality in that it falls short of keeping up with the ever-evolving nature of social media and challenges that stem from it.[17] And yet, the GDPR is the best regulatory policy when it comes to data privacy on the internet to date.

1.1.2 Social Media Cyber Threats

Ample research exists on social media's role in abetting cybercrime such as data theft, cyberbullying, harassment, phishing, online scams, etc.[18] The rapid increase in social media users and social media's integration into daily lives means that more and more personal information becomes vulnerable for malicious actors to access. Lack of regulation has also made social media platforms a medium of choice for terrorist and

[14] Brett Aho, and Roberta Duffield. "Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China." *Economy and Society* 49, no. 2 (May 2020): 1-26. https://sci-hub.se/https://doi.org/10.1080/03085147.2019.1690275.

[15] Aho and Duffield, "Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China," 9.

[16] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz, "We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy." *Paper presented at Network and Distributed System Security (NDSS) Symposium 2019, San Diego, CA, USA, February, 24-27, 2019* (2018): 1-13. https://doi.org/10.14722/ndss.2019.23378.

[17] Degeling et al., "We value your privacy... now take some cookies," 13.

[18] Abdulhamid et al., "Privacy and national security issues in social networks: the challenges." *International Journal of the Computer, the Internet and Management* 19, no. 3 (February 2014): 14-20. https://arxiv.org/ftp/arxiv/papers/1402/1402.3301.pdf

other criminal groups to communicate covertly, recruit, and spread propaganda and disinformation.[19] User surveillance heightens the risk of these cyber threats as it generates even more data, which is then made accessible to third parties that are harder to track and regulate than the social media platforms themselves. Abdulhamid et al. also point out how unregulated use of social media can expose sensitive data associated persons working in state departments and other institutions of import.[20]

It is also an established fact that even states use social media to disseminate propaganda and conduct misinformation campaigns meant to advance their own narrative.[21] These can take the form of inter-state propaganda as one state tries to harm the national image of another or attempts to influence its citizens by feeding them manipulated information.[22] On the other hand, these can also be conducted by the state itself, to advance a certain narrative to its own citizens. This usually happens in the midst of political battles in the wake of elections. Access to in-depth data of social media users again runs the risk of amplifying the effect of such manipulative content. A popular example of this was the alleged Russian interference in the 2016 US elections, which was carried out through targeted social media advertising and information manipulation.[23] Misinformation campaigns have become more targeted and precise as third parties and external data agencies have become more skilled in mining personal data from individuals' social media. This allows actors to disseminate information that is specifically designed to prove most effective against specific groups of citizens' biases and vulnerabilities which are identifiable through data analytics.

[19] Abdulhamid et al. "Privacy and national security issues in social networks: the challenges." 14-20.
[20] Abdulhamid et al. 14-20.
[21] Shabir Hussain, Farrukh Shahzad, and Adam Saud. "Analyzing the state of digital information warfare between India and Pakistan on Twittersphere." *SAGE Open* 11, no. 3 (July 2021): https://journals.sagepub.com/doi/pdf/10.1177/21582440211031905
[22] Hussain, Shahzad and Saud. "Analyzing state of digital information warfare between India and Pakistan on Twittersphere."
[23] Shahzad Hussain and Saud.

In Pakistan’s case, India’s strategic use of media and communication has had a harmful effect on Pakistan’s national image and political interests.[24] This is because India has been effectively using digital media for nation-building strategies[25] and its information campaigns feed into the ruling party, Bharatiya Janata Party’s (BJP) nationalistic Hindu propaganda.[26] Pakistan, on the other hand, does not have a strong digital presence, neither to counter propaganda purported by India nor to develop its own narrative in the digital space. Some effort was made to the latter end during the COVID-19 pandemic when response measures included large-scale digital campaigns and integration of the population onto digitally centralised systems.[27] However, the digital information infrastructure and its policies are still lacking. Pakistan needs a synchronised effort towards information dissemination whereby all state apparatus, including the government, the military, and public offices, are on the same page.[28] There is no comprehensive policy regarding information dissemination or countering misinformation that would take into account the various facets of evolving media and its target audiences.[29] This becomes a more pressing issue as in the absence of a strong national digital presence, Pakistan’s large youth population becomes increasingly acclimatised to the digital space that is dominated by foreign precepts. In his work on transforming national identities and the media, Edensor recognises how exposure to transnational media can lead to proliferation of transnational identities among the youth by undermining their perception of national identity.[30]

[24] Adam Saud and Nehal Kazim, “Disinformation and Propaganda Tactics: Impacts of Indian Information Warfare on Pakistan,” *Journal of Indian Studies* 8, no. 2 (December 2022): 335–54, http://pu.edu.pk/images/journal/indianStudies/PDF/9_v8_2_22.pdf.

[25] Jacobsen, Knut A., and Kristina Myrvold. *Religion and Technology in India*. (New York: Routledge, 2018).

[26] Institute of Regional Studies (IRS), *Fake News: Unravelling the Greater Complexity of How Individuals, Institutions and the Whole Nations Manipulate Facts to Create Fake News to Their Advantage – Book of Peer-Reviewed Papers of International Conference on Fake News and Facts in Our Region Organised by the Institute of Regional Studies in Islamabad on April 24-26, 2019,* (Islamabad: IRS, 2019).

[27] Anwar et al., “Cyber Surveillance and Big Data - Pakistan’s Legal Framework and the Need for Safeguards,” *Research Society of International Law Review* 1, no. 35 (June 2020): 35-61 https://rsilpak.org/wp-content/uploads/2020/06/The-COVID-19-Law-Policy-Challenge-Cyber-Surveillance-and-Big-Data.pdf.

[28] Aqab Malik. "Strategic Communication – A Synchronised Effort for Information Dissemination by Pakistan." *SAGE International*, (2011): https://pdfs.semanticscholar.org/0665/477fa5d7b7fdb50e57cb53112e900ba2b7b7.pdf

[29] Malik. "Strategic Communication."

[30] Tim Edensor, *National identity, popular culture and everyday life* (London: Routledge, 2002).

1.1.3 Current Landscape of Cyber Security in Pakistan

Cyber security is defined as the ability to protect or defend against attacks within the cyberspace, which is inclusive of physical cyber systems and infrastructure.[31] Protecting data and ensuring information accessibility also falls under the purview of cyber security. Syed, Khaver, and Yasin[32] provide an overview of Pakistan's existing cyber security policies. Among the earliest major policies is the Pakistan Electronic Crimes Act (PECA), 2016 which is the first comprehensive legislature that defines a cyber offender and all the various cybercrimes that the offender could be punished for. This includes accessing unauthorised data through hacking, phishing, spreading viruses etc., misuse of data, electronic fraud, cyber-harassment, cyber-stalking, hate speech, use of the internet to abet crimes such as child abduction and others. Notably, the Act also legislated the need to ensure the cyber security of critical infrastructure which includes "information system, program or data that supports or performs a function with respect to a critical infrastructure".[33] The PECA ordained the establishment of a cybercrime investigation agency with its own procedural powers; it set down prosecution and trial terms, and also set rules for possible international cooperation in particular instances of cybercrime. As for preventive measures, the Act gives the federal government jurisdiction to give information systems or service providers directives to take cyber security measures or cooperate in cases of cybercrime as needed. The second measure it proposed was to establish a Computer Emergency Response Team (CERT) which is a recognised establishment in governments across countries that exist to address instances of cyber security breaches and curb threats.[34]

[31] Rubab Syed, Ahmed Awais Khaver, and Muhammad Yasin, "Cyber Security: Where Does Pakistan Stand?" *Sustainable Development and Policy Institute (SDPI) Publications*, working paper no. 167, Islamabad: SDPI, February 14, 2019: 1-15. https://sdpi.org/cyber-security-where-does-pakistan-stand-w-167/publication_detail.

[32] Syed, Khaver and Yasin, "Cyber Security: Where Does Pakistan Stand?" 6.

[33] Government of Pakistan. The Prevention of Electronic Crimes Act 2016. Islamabad: GoP, 2016: 7. https://www.pakistancode.gov.pk/pdffiles/administrator6a061efe0ed5bd153fa8b79b8eb4cba7.pdf

[34] Tughral Yamin, "Cyberspace Management in Pakistan," *Governance and Management Review (GMR)* 3, no. 1 (June 2018): 46-61, https://pu.edu.pk/images/journal/IAS/PDF/4-v3_1_18.pdf.

It was in 2021 that Pakistan’s first dedicated National Cyber Security Policy was published. The policy focuses on addressing the need for a general cyber security governance framework and mechanisms of implementation across the public and private sectors. It highlights the main challenges, namely ownership of cyber security systems, governance structure, enforcement mechanism and excessive reliance on external resources,[35] all of which, strategically speaking, can become a cyberthreat in themselves if not executed properly. The policy does a good job at outlining its main focus, identifying problems and proposing solutions, but it does not go into the specifics of how the policy could be concretely implemented across all sectors to secure the entire national cyberspace. Shaikh points out that the biggest challenges to taking the policy forward are to establish a national cyber security authority that will dedicate itself to policy implementation, achieve an overarching cyber security framework which can be consistently applied to all public and private institutions—most of which are interconnected and overlap when it comes to digital services—establish a cyber security audit team, and develop a specific framework for data protection and privacy.[36] He also mentions how it is a need for Pakistan’s cyber security policy to work towards data sovereignty. While the National Cyber Security Policy appears to consider questions of data protection, implicitly outlines the concept of data sovereignty, it sets very broad and general objectives that fail to address specific threats.[37] For instance, the policy makes no mention of any form of digital surveillance. It does however set down the need to enforce a data protection framework, and it was in 2023 that the Personal Data Protection Bill came to pass. This and the e-safety bill are the first legislations to recognise a need for social media regulation, especially regulation of the social media companies according to

[35] Shaikh, Muneeb Imran. “Pakistan’s Cybersecurity Policy in 2021: A Review.” ISACA, 24 November, 2024. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-39/pakistan-cybersecurity-policy-in-2021-a-review.

[36] Shaikh. “Pakistan’s Cybersecurity Policy in 2021” https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-39/pakistan-cybersecurity-policy-in-2021-a-review.

[37] Ministry of Information Technology and Telecommunication. *National Cyber Security Policy 2021.* Islamabad: MoITT, 2021. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf.

national terms. So far, however, only the final draft of the Personal Data Protection Bill is publicly available, and it will be discussed in this research later.

In 2022, Pakistan's National Security Policy was formally articulated. The policy considered cyber security as a natural part of the nation's national security and emphasised its integral role in protecting critical infrastructure as well as civilian's rights. However, as Khalid[38] notes, it still lacked in crucial ways, specifically in the areas of data protection and the development of a digital surveillance capability to combat disinformation and influence operations. With regards to data collection, the most promising step taken was the implementation of information technology services and systems such as the National Database and Registration Authority's (NADRA) interconnected national database that maintains the largest record of its citizens' data sourced from across all state departments.[39] However, NADRA and other sensitive national offices, such as the Prime Minister's Office have faced cyber-attacks as recently as in 2022, which suggests that the present infrastructure is not yet up to the mark.

Pakistan's very own cyber response team was finally legislated in October 2023, through the CERT Rules 2023. The rules formally call for the establishment of CERTs at the national, sectoral and organisational levels as well as a CERT Council which will be consultative in nature. The CERT's mechanisms are meant to ensure awareness and preemption of cyber threats through research and developments, audits of existing systems and, most crucially, incident response services. The CERT Rules are an exemplary legislature in Pakistan's nascent cyber security landscape. If implemented well, it has the potential to arm the nation with a proactive cyber defence system. However, the issue of social media cyber threats does not fall under the purview of the CERT.

[38] Khalid, Zaki. "Examining the national security policy of Pakistan 2022-2026". *Centre for Strategic and Contemporary Research.* 2022. https://cscr.pk/explore/themes/defense-security/examining-the-national-security-poliensure the cy cy-of-pakistan-2022-2026/
[39] Syed, Khaver and Yasin, "Cyber Security: Where Does Pakistan Stand?" 10.

An overview of Pakistan's existing cyber security policies reveals that in the past few years, there has been a significant increase in attention to cyber security which is evident in the development of three different policies over the past three years as well as the inclusion of cyber security in the National Security Policy 2022. However, as of yet no concrete steps have been taken to implement the policies or even introduce concrete plans. Several researchers and security experts have been studying Pakistan's current cyber security needs and have presented analyses of existing policies. Moreover, as the cyberworld is one in constant flux and evolvement, it appears that current policies are far behind in terms of keeping up with advancing technology and their unique challenges. Not a single policy directly addresses the vital issue of data protection and user privacy on the internet, let alone the threat that social media user surveillance poses to them, save for the recently released final draft of the Personal Data Protection Bill. This bill, too, has been criticised by experts and labelled as impractical, and a performative act.

1.1.4 Social Media Intelligence

Another aspect of security in the age of social media and big data is the emergence of intelligence-gathering through social media, which is now considered essential for national defence. After the traditional practices of human intelligence (HUMINT) and technical intelligence (TECHINT) with its subcategories of imagery, signals, communications, and electronic intelligence, technological advancement has introduced newer forms of intelligence such as hacking intelligence[40] and social media intelligence (SOCMINT).[41] SOCMINT is based on mining social media users' data and analysing it for intelligence.[42] It is used in a number of ways, such as for encouraging social cohesion, which China has attempted through its Social Credit System, and for predictive detection

[40] Philip HJ. Davies, "Intelligence, information technology, and information warfare," *Annual Review of Information Science and Technology* 36 (2002): 313-52. https://sci-hub.se/https://doi.org/10.1002/aris.1440360108.

[41] David Omand, Jamie Bartlett, and Carl Miller. "Introducing social media intelligence (SOCMINT)," *Intelligence and National Security* 27, no. 6 (July 2012): 801-823. https://sci-hub.se/https://doi.org/10.1080/02684527.2012.716965.

[42] Omand, Bartlett and Miller, "Introducing social media intelligence (SOCMINT)," 802.

of potential criminal activity.[43] Lim highlights how big data analytics, together with traditional, human-centred intelligence can provide a much more nuanced and holistic means to gather necessary information on certain groups.[44] He argues that a comprehensive legal framework that sets down the ethics of SOCMINT and effective accountability mechanisms for authorities in charge of it would allow successful use of data collected from social media not only for intelligence but to inform better policy and intervention. It can also help identify social trends or patterns which may hint towards imminent events such as the onset of a disease or infection.[45] In this evolving technological climate, it is evident that Pakistan needs to address its policy gaps regarding information security so it can effectively defend itself against emerging threats as well as utilise newer sites of information and forms of intelligence for its own strategic ends.

1.1.5 Literature Gap

There is a good amount of research on the general topic of social media and cyber security threats that cover cybercrime committed by individual actors who abuse the online platforms' features. This includes cyber harassment, hacking, phishing, identity and data theft, data leaks, organisation of terrorist and criminal activities, etc. Research that specifically focuses on social media surveillance and its challenges, especially in terms of the social media companies' policies and use of user data, is limited. Certain studies highlight the issue by including social media surveillance as one type of surveillance that comes under the vast umbrella of cyber surveillance. Research has also focused on the legality of social media companies' surveillance practices in terms of civilians' privacy and human rights violations. This is further reflected in studies done on exemplary policies such as the GDPR and the national surveillance practices of the Chinese government. In fact, critique of China, North Korea and others that are not open to Big Tech social media companies'

[43] Aho and Duffield, "Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China," 2.
[44] Kevjn Lim, "Big data and strategic intelligence," Intelligence and National Security 31, no. 4 (June 2016): 619-635. https://sci-hub.se/https://doi.org/10.1080/02684527.2015.1062321.
[45] Omand, Bartlett and Miller, "Introducing social media intelligence (SOCMINT)," 803.

establishment in their region, is one of the rare cases in which social media surveillance has been studied in relation to national security. Overall, there appears to be a literature gap when it comes to understanding the threats of social media as a national security concern. This research aims to do so specifically in the context of Pakistan, where there seems to be a dearth of research in the field of internet surveillance and cyber security that should be understood as essential to the country's national security strategy.

1.2 Hypothesis

Pakistan can counter cyber security threats posed by social media user surveillance through effective cyber security policy.

1.3 Research Questions

- What are the cyber security threats that emerge from social media user surveillance?
- How effective is Pakistan's existing regulatory policy against cyber security threats posed by social media?
- Why does Pakistan need effective policy to address threats which emerge from social media user surveillance?

1.4 Research Objectives

- To discuss cyber security threats that emerge from social media user surveillance.
- To highlight gaps within Pakistan's existing cyber security policies in terms of its effectiveness against social media user surveillance.
- To sensitise the need for effective Pakistan's cyber security policy.

1.5 Theoretical Framework

This research will apply realism as its overarching theoretical framework to better contextualise the challenges of social media user surveillance as a threat to Pakistan's national security. In particular, realism's principle of national sovereignty best complements this research's key concept of digital and data sovereignty.

In the domain of international relations, the theory of realism sees nation-states as self-interested, sovereign entities that are purely motivated to act in the favour of their own security in an anarchic world, that is, one where there exists no central authority. In such a world, it is each nation's prerogative to look out for its own national interests, foremost of which is its national security. Cyber security has now long been identified as a national security issue, and has in fact, been linked with the realism framework to understand cyber politics between nations and the concept of sovereignty in cyberspace.[46]

Interestingly, when the internet first emerged as a publicly accessible global space, several enthusiasts believed that the unregulated digital-scape, unbound by territorial borders could actually overturn state sovereignty.[47] However, as the internet would go on to develop in a world unable to break free from what the realist would call its 'natural' order of anarchy and self-service, it eventually lent to a cyberworld that is very much subject to state governance. This is evident in how various cyber threats have been linked to national security through research and policy as vital security concerns for individual states,[48] which have responded by developing their own cyber security policies in the past

[46] Anthony Craig and Brandon Valeriano, "Realism and cyber conflict: Security in the digital age," in *Realism in Practice: An Appraisal*, ed. by Davide Orsi, J. R. Avgustin and Max Nurnus (Bristol: E-International Relations, 2018), 85-101. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

[47] Julia Pohle, and Thorsten Thiel, "Digital sovereignty," *Internet Policy Review* 9, no.4 (December 2020). https://policyreview.info/concepts/digital-sovereignty

[48] Holger Stritzel, "Securitization and The Copenhagen School," In *Security in translation: Securitization theory and the localization of threat,* edited by Stuart Croft (London: Palgrave Macmillan, 2014): 11-36.

few decades.[49] Researchers Hansen and Nissenbaum[50], who have extensively worked on positing threats which emerge from the cyberspace as security issues. This includes challenges related to internet safety, data mining, surveillance and more.

The core concept underlying the essentiality of national cyber security, and by extension the issue of surveillance and data extraction from individuals on a mass level is best explained by the realism framework. Data, including personal details and sensitive information, defining characteristics of regional, ethnic, and minority groups, users' real-time activities and location, all of which can be strategically used against groups of people by nefariously motivated actors. This alone makes citizens' data an undoubtedly invaluable national asset.[51] From a realist perspective, each state must protect its citizens', and its institutions' data from being captured and manipulated by foreign organisations, including global corporations and intelligence agencies. The concept of data sovereignty aptly applies here, whereby the state should have control over how its citizens' data is being handled, where it is being stored and shared, and what use is being made of it. This is also imperative for preventing cyber warfare, specifically, disinformation campaigns and behaviour manipulation agendas such as the Cambridge Analytica episode of influencing US voters.[52] The idea of data sovereignty—and by extension, digital sovereignty—falls in line with the realism framework as it envisions the global cyberspace divided into territorial blocs, wherein each state has its own regulatory establishment to keep its digital and digitally connected critical infrastructure secure.[53] These blocs are not a reflection of on-ground territorial boundaries as states extend their

[49] Max Edgar Floris Geelen, "Cyber Securitization and Security Policy" (Master's diss., Leiden University, 2016). https://studenttheses.universiteitleiden.nl/access/item%3A2663862/view

[50] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1155–75. https://academic.oup.com/isq/article/53/4/1155/1815351.

[51] Liu, "The Rise of Data Politics: Digital China and the World," *Studies in Comparative International Development* 56 (March 2021): 45-67. https://link.springer.com/article/10.1007/s12116-021-09319-8.

[52] Candace L. White, and Brandon Boatwright, "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations," *Public Relations Review* 46, no. 5 (December 2020): 1-7. https://www.sciencedirect.com/science/article/abs/pii/S0363811120301077.

[53] Wuhan University et al., "Sovereignty in Cyberspace: Theory and Practice (Version 4.0)," *World Internet Conference*, January 16, 2024. https://subsites.chinadaily.com.cn/wic/2024-01/16/c_956165.htm.

jurisdiction beyond borders to regulate data controllers such as social media companies and exercise control over its citizens' data.[54]

Social media's data collection policies are already perceived as a concern in Pakistan at least to some degree. This much is evident in the passing of the e-safety and data protection bills, which will be further discussed and critically analysed in this study. Applying the theoretical framework of realism together with the key concepts of data and digital sovereignty—both of which have become increasingly more relevant with the development of the data economy—will help identify what is lacking in existing policy.[55] It will further illustrate the crucial need and the specific requirements of a comprehensive data policy in Pakistan, one that especially caters to the challenges of social media user surveillance.

1.6 Significance

The significance of this study lies in its potential to expand research and literature on internet surveillance in the specific area of social media surveillance. It will outline the ever-evolving contours of social media surveillance, its perceived threats and even possible advantages that can be achieved if proper policies are put into place. This study will also prove significant because it will critically analyse some of the most used and biggest social media platforms' policies. This method can be applied to critique other social media platforms, websites, applications, and internet services' privacy policies as well. In fact, the entire study could provide a basis for further research into user data protection policies and internet surveillance practices in different sectors. Opening this avenue of research may help establish the overall challenge of understanding user data and privacy protection as well as devise appropriate and effective policies for them.

[54] Vatanparast, Roxana. "Data governance and the elasticity of sovereignty." *Brook. J. Int'l L.* 46 (May 2021): 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839847

[55] Su and Tang, "Data Sovereignty and Platform Neutrality – A Comparative Study on TikTok's Data Policy." *Global Media and China* 8, no. 1 (February 2023): 57-71. https://journals.sagepub.com/doi/full/10.1177/20594364231154340.

Another pertinent feature of this study that adds to its significance is its application of the realism theoretical framework to understand social media surveillance and data collection as a cyber security threat that is crucially linked to national security. Doing so, allows us to explore the concepts of data and digital sovereignty, which are essential in drafting effective policy for the security of Pakistan's cyberspace. This will further prove significant in expanding the scope of cyber security issues on a personal level for civilians as well as at the institutional and national level. Finally, this study is most significant for Pakistani literature on cyber security research because it is one of the few of its kind, in that it discusses the seldom explored issue of data privacy and social media user surveillance.

1.7 Research Methodology

This research will use qualitative research methods to explore its questions and fulfil its objectives. Qualitative research helps understand a problem through a holistic lens by taking into consideration descriptive data, such as text, social conditions, experiential accounts of research subjects, and more.[56] It allows critical investigation of topics that cannot be reduced to or measured by numbers alone, such as lived experiences of unique communities and their cultures. Within qualitative research there is more room for researching a topic from different angles instead of studying only a few of its aspects in isolation. Ethnographic research for instance is meant to study the culture, behaviour, socialisation and other details of a subject or group of subjects through multiple methods instead of focusing on a singular characteristic of the subject. This kind of research lends to a deeper understanding of its subject.[57] As this research is focused on understanding and defining social media surveillance as a feature on its own and a cyber security threat while studying the effectiveness of regulatory policy, a qualitative research method approach will prove most appropriate. This thesis also endeavours to highlight gaps

[56] Lorrie R. Gay and P. Airasian, *Educational research: Competencies for analysis and applications* (New Jersey: Pearson, 2016).

[57] Martyn Hammersley, "Ethnography: problems and prospects," *Ethnography and education* 1, no. 1 (March 2016): 3-14. https://www.tandfonline.com/doi/full/10.1080/17457820500512697.

within Pakistan's existing cyber security policies that fall short of addressing emerging cyber security threats posed by social media user surveillance. It will do so by critically analysing various policies (specified below), which by nature is a qualitative research method.

1.7.1 Research Design

This research will employ an exploratory design which is best suited for studying a less-explored topic area. Its purpose is to get a comprehensive and detailed understanding of the research question. It typically includes the use of multiple methods and sources for thorough investigation. This research will refer to both primary and secondary data, including privacy policies of social media companies, law related to data protection, privacy rating reports as primary material and books, journal articles, and statistical reports as secondary sources. An exploratory design comes with the benefit of freedom to study different aspects of the main thesis question. On the one hand, while it attempts to explore the link between social media user surveillance and cyber security threats in general, it will also link it with Pakistan's national security and civilians' privacy rights. Moreover, it will also critique the effectiveness of Pakistan's existing social media regulation policies. This study then requires a multi-level research to come to an informed conclusion regarding its thesis statement and this is best complemented by an exploratory design. Additionally, this particular design is most suited for research for which data collection may prove to be a challenge. It is understood that in the case of social media platforms', it is expected of them to not be entirely transparent in terms of company practices and policy. Similarly, policies of organisations directly related to data surveillance in Pakistan, such as NADRA, and other sensitive departments are not accessible. For instance, while the parliament has passed the Personal Data Protection Bill in 2023 and talked about its supposed social media regulation policy, this bill has not yet been made public. Therefore, this research will have to rely on appending what can be found in primary sources with other secondary sources to come to a better understanding of the thesis.

1.7.2 Data Collection Methods

Critical analysis is a method by which a piece of document or an artefact is systematically analysed to be better understood and critiqued. In this research, social media privacy policies of selected platforms and Pakistan's cyber security policies will be critically analysed to establish from the former, an understanding of standard social media user privacy and data collection processes. This will be accompanied by an overview of existing research and other relevant material, such as reports measuring Facebook and YouTube's standard of privacy. Secondly, analysis of Pakistan's cyber security policies will allow an understanding of how existing policies address the cyber security concerns that emerge from social media user surveillance and what are the policy gaps.

The data collection method used in this study will be a critical analysis of the privacy policies of selected social media companies, namely, Facebook and YouTube. The social media sites have been chosen on the basis of their usage in Pakistan. Each of the social media sites selected rank among the ten most used platforms.[58] Since these sites are among the most popular, their policies and practices naturally become the set standard for social media policies. The privacy policies of each of these platforms are published and accessible online for user perusal. The privacy policies' analysis will be accompanied by a critical analysis of Pakistan's existing cyber security policies, specifically, the e-safety bill, which is the first to include social media regulation clauses.

Analysing privacy policies of social media platforms will provide primary evidence for the existence of social media user surveillance. It will help define the different forms this kind of surveillance takes and the extent to which it goes. It will also allow insight into how the policies are framed and worded, and how transparent and accessible they are for the average user. Secondary research available on the topic and other sources, such as the

[58] Pakistan Telecommunication Authority. Annual Report 2023. (Islamabad: PTA, 2024) https://www.pta.gov.pk/assets/media/pta_annual_report_12022024.pdf.

legal proceedings of cases against Facebook reveal certain features of user surveillance that platforms may or may not have admitted to. Since, this research will be studying the policies of two different platforms, a collective analysis could point out commonalities between each and hence define what constitutes standard social media user data and privacy policies. Secondly, this study will analyse Pakistan's cyber security policies in light of the previous analysis' findings so that their shortcomings and gaps in terms of social media regulation may become apparent. As discussed in the literature review section, the main cyber security policies in Pakistan to date are PECA, CERT, a section in the National Security Policy 2021, and the recently passed Data Protection and e-safety bills. Of these, the last two are the only ones that directly include clauses pertaining to social media regulation. However, since the Personal Data Protection Bill hasn't yet been published for the public, secondary sources will have to be relied on. In this case, the e-safety bill will become the main document of analysis.

1.7.3 Data Analysis Techniques

The analysis of the selected social media companies, Facebook and YouTube's privacy policies will primarily seek to i) what data each platform collects and how each does it, ii) how data is processed and who has access to it? iii) how data is stored and transferred and iv) what are their consent and transparency procedures? Once answers to these questions have been extracted from each platform's policy, the results will be analysed for commonalities as well as any differences that stand out.

Moreover, Pakistan's cyber security policies will be analysed for clauses that directly relate to user data, data collection, data privacy, social media, and internet and social media surveillance. The analysis will help arrive at an overview of how well Pakistan's cyber security discourse comprehends and frames the issue of data privacy and social media user surveillance. Finally, a side-by-side comparison with the findings of the social media platforms' privacy policies' analysis will reveal the extent to which Pakistan's cyber security policies actually address potential threats posed by social media user surveillance and furthermore, how it is lacking.

1.8 Organisation of the Study

The first chapter of this thesis will focus on deciphering the cyber security threats that emerge from social media surveillance. This will include references to secondary research and other sources that define and explain social media user surveillance and the ways in which it exists. This will be followed by individual critical analyses of each of the four selected social media platforms' privacy policies. The chapter will conclude by comparing the findings from each analysis and a collective understanding of social media platforms' data and privacy policies.

The second chapter will then attempt to outline why it's necessary for Pakistan to address these threats. It will do so by critically analysing Pakistan's existing cyber security policies and examining any attempts at social media regulation that these have included. Findings from the previous chapter will further help define the shortcomings of existing policies by highlighting how they fail to address the challenges and threats posed by social media user surveillance.

The last chapter will present a summary of the study and its findings, followed by its analysis and finally a discussion which will help understand the results of this study in light of its theoretical framework and research objectives. This section will refer to the research's findings to evaluate the hypothesis of this study and give comprehensive answers to the research questions. It will conclude with an exploration of the future scope of this study and how its findings could be taken and applied to further research to advance the understanding of cyber security and internet surveillance in general, but also specifically contribute to the research areas of social media user surveillance and data policy.

Chapter 2

CONCEPTUAL FRAMEWORK OF THE STUDY

This chapter will discuss the conceptual framework of the study. The conceptual framework for this research is Shoshana Zuboff's concept of surveillance capitalism, which sits at the heart of the problem that this study tackles. To understand social media user surveillance—what it is, why it is, how it currently exists and continues to evolve into complex challenges for the future—it is first important to understand the economic model that fosters it. This economic model and the political economy it relates to has been termed surveillance capitalism, which can also be understood by the term data economy. This chapter will, in particular, address the first research question posed by this thesis; that is, what are the cyber security threats that emerge from social media user surveillance. Through an explanation of the conceptual framework and its application to the topic at hand, we can better understand the implications of social media user surveillance.

2.1 Surveillance Capitalism

The story goes that man found land to be a resource and exploited it to the point that it now runs short and hangs at the brink of catastrophe. Since the capitalist economic order is based on a primary chase for profits, gleaned from whatever it takes, it is no wonder that when man uncovered an abundant resource in the form of data, opportunities to capitalise upon it naturally abounded. Zuboff posits that data from various sources has become the modern most-in-demand raw material that corporations and agencies from all sectors rely on to maximise profit and collect vital information from.[59] However, if data—and, to be precise, human data—is the raw material, then the resource to be extensively farmed under the tenets of capitalism is the human being itself. More specifically, the human brain, human thoughts, human behaviour and actions all become commodifiable

[59] Zuboff. *Age of surveillance capitalism.*

and for the taking under the surveillance capitalism regime. This practice of treating individuals as sites for mining units of profitability undoubtedly poses a multitude of complex ethical, moral and practical questions that need to be addressed through a thorough understanding of how this process works.

While this research is focused on social media and its data use, surveillance and collection of user data has become a natural part of all sectors, including finance, healthcare, telecom, retail, and businesses not even directly related to online services.[60] Of course, in a lot of ways, the availability of detailed data that can be both continuous and discrete depending on how it is processed, is valuable. Healthcare institutions use client or patient data, to make important inferences that can help with diagnoses, personalised medication plans, gauge treatment effectiveness, and provide various insights that can inform best health practices.[61] An illustrative example is Pakistan's use of citizens' data during the COVID-19 pandemic to track the incidence of the virus and vaccination needs[62]. However, the surveillance capitalist model is not restricted to data collected for improving essential services, but it has, in fact, become the norm for various corporations. This means that businesses are incentivised to collect all forms of data they can get without plausible cause or informed consent of clients. This data extends anywhere from voluntarily submitted information when signing up for services (like names, email addresses, contact numbers, and home addresses, among others) to metadata that may be accessed by the service provider without users' awareness.[63] Metadata includes websites that track user browser history, how long a user spends on a web page, the position of the user's clicks on the page, and other data points that are compiled into a database of user profiles, which help personalise the user's experience, but also enable third-party

[60] Lim, "Big data and strategic intelligence," 4.

[61] Joachim Roski, George W. Bo-Linn and Timothy A. Andrews, "Creating value in health care through big data: opportunities and policy implications," *Health affairs* 33, no. 7 (2014): 1115-1122. https://sci-hub.et-fine.com/10.1377/hlthaff.2014.0147

[62] Atta Ullah, Chen Pinglu, Saif Ullah, Hafiz Syed Mohsin Abbas, and Saba Khan, "The role of e-governance in combating COVID-19 and promoting sustainable development: a comparative study of China and Pakistan," *Chinese Political Science Review* 6, no. 1 (November 2021): 86-118. https://link.springer.com/article/10.1007/s41111-020-00167-w.

[63] Zuboff, *Age of surveillance capitalism*.

advertisers to show users targeted ads.[64] Metadata also constitutes more sensitive information, such as IP addresses, the user's device model, their location and other information linked with the user's device that is easily accessible to mobile network providers, or to any website using 'cookies' to track users.[65] This data can then be sold to advertisers[66] as well as state and other intelligence agencies without the user's knowledge.[67] From the researcher's personal example, visiting a mall in her city automatically led her to receive a text message from her network provider when she entered the mall parking, which notified her that she had been awarded free mobile data for choosing to go to that particular mall. So, clearly, in this case, the network provider was using at least its clients' geolocation data for purposes beyond those that they had been informed about or had agreed to. To truly understand why this level of data access being available to companies can pose a major threat, it is important to consider that, in most cases, clients or users of a service do not have control or awareness over which of their data is being surveilled, collected, how it is processed, and who it is shared with. The lack of a proper policy or legal framework only exacerbates the problem.

2.1.1 Big Data Analytics and Social Sorting

The scale at which the data economy has expanded, and the sheer amount of data being produced has led to the establishment of the big data industry. Big data is not only known for its large volume but its variety and the velocity at which big data analytics can process raw data.[68] The swathes of raw data and databases being generated through digital

[64] Andreas Kuehn, "Cookies versus clams: Clashing tracking technologies and online privacy." *info* 15, no. 6 (September 2013): 19-31. https://sci-hub.et-fine.com/10.1108/info-04-2013-0013.

[65] Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique," 3.

[66] Damion Mitchell, and Omar F. El-Gayar, "The effect of privacy policies on information sharing behavior on social networks: A Systematic Literature Review." Paper presented at the *53rd Hawaii International Conference on System Sciences, Maui, Hawaii, USA, January, 7-10, 2020*. https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1230&context=bispapers

[67] Ian Brown. "Social media surveillance." 2015. https://onlinelibrary.wiley.com/doi/full/10.1002/9781118767771.wbiedcs122

[68] Roski, Bo-Linn and Andrews, "Creating value in health care through big data: opportunities and policy implications," 1115-1122.

systems such as social media platforms, applications, the internet at large, communication devices and other smart objects that now comprise the entire gamut of the Internet of Things (IoT) is referred to as big data. The data on its own does not mean much, so, to take it a step forward, processing systems based on machine learning and the science of data analytics sort through the data, arranging it into sets of comprehensible information and extracting meaningful inferences. These inferences can relate to patterns in user behaviour, their preferences, and even their sentiments or state of mind. Omand notes the application of 'sentiment analysis', whereby textual data such as in social media posts is processed to identify certain qualities that are telling of users' emotions.[69] So, in addition to just voluntarily submitted data—which, by the way, is not entirely 'voluntarily' since many essential services are withheld unless certain information is given up—and metadata, analyses are also performed on user data to acquire even more knowledge about users through a process in which they do not directly participate in. This is known as social sorting.

2.1.1.1 Prevalence of Bias in Social Sorting

There is ample evidence that suggests problems with how such data processing methods and social sorting can exhibit biases, since any data point is only a singular fact about an individual that may not be truly representative when taken out of context and considered in isolation. An example of this is the use of big data analytics in predictive policing, which is a method used by certain police departments to pre-empt crime through algorithm-based data processing of past crime records, reports, demographic data, etc.[70] However, researchers have identified bias against people of colour in the case of the US justice system's use of predictive policing tactics as the algorithm assigned white criminals lower recidivism scores than others.[71] While work is continuously being done to improve data processing algorithms and experts call for combining offline, contextual

[69] Omand, Bartlett and Miller, "Introducing social media intelligence (SOCMINT)," 810.
[70] Minocher and Randall, "Predictable Policing," 4.
[71] Minocher and Randall, 4.

data along with machine-derived analytics for more representative results,[72] the fundamental problem of reducing individuals to mere data points will remain. Especially because the data is not only used to collate information provided by users but, as we will see in the next section, to further generate data that is fed back to users in various forms, thereby creating a loop where characteristically limited information is being recycled and reinforced. Minocher and Randall illustrate this well by stating, “Big data surveillance obviates local histories, peoples, and experiences in order to render a particular perspective for controllers and users of these big data-driven systems”.[73]

To be clear, big data and data analytics have allowed advancements in many areas and opened up many avenues for acquiring important information that has led to increased knowledge and innovations. For instance, Roski, Bo-Lin and Andrews identify many ways the healthcare sector can benefit from use of big data in terms of potential cost reduction in the billions.[74] They also note that, among other improvements to medical treatment, big data analytics have led to the discovery of certain patterns in patient histories that may have been missed otherwise. In particular, they mention the Durkheim project, which was a collaboration between Veterans Health Administration and Facebook that used real-time prediction to analyse voluntary, opt-in data from veterans' social media accounts and mobile phones for suicide risk prevention.[75] In Pakistan's context too, a number of studies have looked into how machine learning algorithms applied to datasets collected during the COVID-19 pandemic can help with virus detection, classification and categorisation, incidence prediction and more.[76] Similarly,

[72] Omand, Bartlett and Miller, "Introducing social media intelligence (SOCMINT)," 801-823.
[73] Minocher and Randall, “Predictable Policing,” 3.
[74] Roski, Bo-Linn and Andrews, "Creating value in health care through big data: opportunities and policy implications," 1115-1122.
[75] Roski, Bo-Linn and Andrews, 1115-1122.
[76] Mazhar Javed Awan, Muhammad Haseeb Bilal, Awais Yasin, Haitham Nobanee, Nabeel Sabir Khan, and Azlan Mohd Zain, "Detection of COVID-19 in chest X-ray images: A big data enabled deep learning approach," *International journal of environmental research and public health* 18, no. 19 (September 2021). https://www.mdpi.com/1660-4601/18/19/10147; Ayoub et al., "Classification and categorization of COVID-19 outbreak in Pakistan," *Comput Mater Continua* 69 (January 2021): 1253-69. https://www.researchgate.net/profile/Mustufa-Abidi/publication/352130166_Classification_and_Categorization_of_COVID-

big data has proved to be very advantageous in several public service fields, such as public policy, urban design, traffic control, crime and others.

For the big data industry and social sorting models to truly prove successful, what is required is a steady flow of more and more data. This means that data brokers and those that happen to sit on vast reserves of data as a by-product—that is, social media companies—have an incentive to engage in exploitative surveillance tactics. The problem is not big data itself but that, under a surveillance capitalism model, the personal data of individuals is a lucrative asset, which, without established ethics in the trade and the lack of adequate policy, becomes a detriment to human rights as well as security.

2.1.2 Social Media Surveillance

This research is focused on data collection and surveillance practices enabled through social media platforms, specifically by social media companies themselves. Integral to understanding social media user surveillance is acknowledging that these companies are multinational, multibillion businesses that monopolise the technological industry in several areas. Meta—the company behind Facebook, Instagram, and WhatsApp WhatsApp—and Google, which, aside from being the world's leading search engine, owns YouTube and a range of other essential online services, are both among the highest revenue-raking companies in Big Tech. Meta, which is also the largest social media company, reported a total revenue of 40.1 billion USD for the year 2023 with a total of 3.98 billion active users from across the world.[77] Alphabet, the parent company of Google, on the other hand, made more than 297.132 billion USD in revenue in the same

19_Outbreak_in_Pakistan/links/60bc6768299bf10dff9c89fb/Classification-and-Categorization-of-COVID-19-Outbreak-in-Pakistan.pdf; Saba Noor, Waseem Akram, and Touseef Ahmed, "Predicting COVID-19 incidence using data mining techniques: a case study of Pakistan," *Broad Research in Artificial Intelligence and Neuroscience* 11, no. 4 (February 2020): 168-184. https://www.researchgate.net/publication/347858382_Predicting_COVID-19_Incidence_Using_Data_Mining_Techniques_A_case_study_of_Pakistan

[77] Meta. "Meta Reports Fourth Quarter and Full Year 2023 Results; Initiates Quarterly Dividend." Meta Press Release, February 1, 2024. On the Meta website. https://investor.fb.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx.

year.[78] According to current valuations, both Meta and Alphabet rank among the top ten in terms of most valued companies in the world. Although this research only includes YouTube as one of the social media companies studied and not Google or Alphabet in its entirety, the parent company's valuation and access to a vast user base directly benefits the video-sharing platform as well. The reason these figures matter is because they reflect the companies' position in the industry, which not only shows their massive influence but also their access to data. Meta's billions of users allow it access to a continuous supply of massive amounts of data and control over users' experiences and what information they receive.[79] Additionally, these companies are pioneers in the social media industry and of various online services such as Google Earth, Google Maps, and the expansive Google Suite. Moreover, they continue to head many kinds of technological innovations, such as Meta's foray into virtual reality (VR) experiences. This illustrates, that these corporations make good profit off of services that are primarily free of cost for users, except for the personal data they must pay in.

In 2012, Facebook (which was the company's name before it became Meta) acquired the photo-sharing app, Instagram, which did not value much at the time next to Facebook itself. In the following decade, Facebook would go on to acquire a host of smaller companies, including the popular messaging app, WhatsApp, Oculus VR, and Giphy, an underdeveloped site dedicated to GIF sharing. Zuboff highlights how these acquisitions helped Facebook beyond eliminating potential competition, by giving it access to the most valuable ingredient: more data.[80] WhatsApp currently has two billion active users around the world, and unlike Facebook where users share content in the form of occasional text and multimedia posts, the instant messaging app gets more personal. WhatsApp is where users have their day-to-day conversations with loved ones, peers and professional contacts. While Meta claims that it does not read private chats, this is

[78] Alphabet. "Alphabet Announces Fourth Quarter and Fiscal Year 2023 Results." Alphabet Earnings Release, January 30, 2024. On the Alphabet website. https://abc.xyz/assets/95/eb/9cef90184e09bac553796896c633/2023q4-alphabet-earnings-release.pdf, accessed February 5, 2024.

[79] Trottier, Daniel. "A research agenda for social media surveillance." *Fast Capitalism* 8, no. 1 (2011): 59 - 68.

[80] Zuboff. *Age of surveillance capitalism*.

contested and will be discussed later in this chapter. In any case, having access to different social media applications and websites allows the company greater coverage. Many people use multiple social media platforms, each to engage with different contacts and for different purposes. So, for instance, Facebook at least has knowledge of a user's different contacts on different platforms among other openly visible information. Instagram is populated by users who are younger and do not use Facebook as much,[81] which means that the app allows Meta access to an even wider demographic and more users worldwide. Similarly, this research discusses Alphabet or Google applications above because their vast portfolio allows them greater access to data, which ultimately helps optimise and run a social media site like YouTube through algorithms that become better at predicting which content and ads to push towards each user.

2.1.3 Data Collection

The different ways in which social media companies collect user data will be discussed in detail when critically analysing each of their privacy policies. However, there is also a lot of research on this topic that helps understand what isn't explicitly stated in official policy documents. Social media companies generally use all the same data collection methods discussed above for websites such as tracking cookies, which allow them to monitor and gather user details from across the internet, and even devices. Social media as well as other applications can also access all contacts saved within a device, photos in the gallery, the device's camera and microphone. Many features require user permissions, however, since functionality of the social media app gets progressively limited as users restrict actions, they are discouraged from disabling access by design. The complexity of understanding company policy and privacy settings also acts as a disincentive and most

[81] Kemp. *Digital 2023: Global Overview Report.*

users choose to work with default settings.[82] Moreover, Kroger and Raschke,[83] discovered through in-depth study, that just because a user has disabled access, it does not mean that the permissions cannot be overridden by the device system itself or malicious code running through other apps. In fact, they also looked into how devices actively ‘listen-in’ to their surroundings. They found that mobile phones are able to pick sound vibrations from their surroundings that can be run through programmes that allow certain spoken words to be identified. Health tracking apps are able to gather minute data like when a user goes to sleep, and how well they slept the past night, including when they entered REM or NREM sleep. This suggests that motion sensors and other built-in technology within devices are able to track user behaviour and details.[84] In fact, Zuboff[85] cites in her research that certain devices such as the Samsung Smart TV which uses the Android operating system was recording full conversations spoken in its vicinity. The recordings picked up personal information such as news about a user’s pregnancy, their life plans, and something as sensitive as their contraction of a rare disease. This indicates that any app, including social media can potentially use device features, like microphones, for invasive surveillance and gather personal health data about the user as well as their entire conversations, if they are able to bypass the phone’s security system. This then suggests that it’s not entirely impossible that social media apps may be collecting information about users’ offline activity as well. In any case, malicious apps and hackers always pose a potential threat of accessing device features for surveillance and theft of data. Additionally, data processors and brokers also use “data mining”, a pattern-finding process which helps determine more in-depth details about users, which a times, can even

[82] Carey Wong, "Smartphone location-based services in the social, mobile, and surveillance practices of everyday life," *Media@LSE MSc Dissertation Series* (2014): https://www.lse.ac.uk/media-and-communications/assets/documents/research/msc-dissertations/2013/96-Wong.pdf.

[83] Jacob Leon Kröger and Philip Raschke. "Is my phone listening in? On the feasibility and detectability of mobile eavesdropping," In Data and Applications Security and Privacy XXXIII: 33rd Annual IFIP WG 11.3 Conference, DBSec 2019, Charleston, SC, USA, July 15–17, 2019, Proceedings 33, pp. 102-120. *Springer International Publishing*, 2019.

[84] Quinn Grundy, Lindsay Jibb, Elsie Amoako, and Geoffrey Fang. "Health apps are designed to track and share." *bmj* 373 (June 2021): https://www.bmj.com/content/373/bmj.n1429.

[85] Zuboff. *Age of surveillance capitalism*.

take on a predictive quality as it can forecast user's preferences[86] or behaviour.

2.1.4 Advertisement-based Revenue Model

Speaking of social media companies, in particular, it is important to note their revenue model, which is largely based on selling third-party advertisers user profiles and attention. Most notably, platforms like Meta are not simply selling ad space[87] as YouTube does, instead, they are selling detailed user profiles to advertising agencies. Advertisements have always worked this way. Their success rate depends on how much they know about the consumer, their habits, preferences, the demographic they belong to, financial status, all such details can help market a product in a more targeted way to each consumer. When Facebook started out, it was actually opposed to an advertisement-based revenue model and used data collected from users simply to optimise its own services. As the platform grew, it began to accumulate so much data that it could aptly be described as a 'behavioural surplus'.[88] As with any surplus, this too has to be sold for a profit, and thus user data became a commodity for sale. Considering that there is a lack of regulation policies for social media user surveillance even in the most developed countries, and that third-party data brokers operate in "secrecy outside of statutory consumer protections",[89] it would be quite naïve to believe that companies don't do whatever they can to surveil users and gather maximum data. This can include bypassing permissions. As Degeling et al.[90] uncovered in his research, even websites that ask users to consent to cookie tracking often start gathering data before the user can select an option. Moreover, websites and

[86] Xu, Lei, Chunxiao Jiang, Jian Wang, Jian Yuan, and Yong Ren. "Information security in big data: privacy and data mining." *Ieee Access* 2 (October 2014): 1149-1176. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6919256

[87] White and Boatwright. "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations."

[88] Zuboff. Age of surveillance capitalism. 74.

[89] White and Boatwright. "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations." 3.

[90] Degeling et al., "We value your privacy... now take some cookies," 2.

applications have built-in extensive tracking capabilities even without the use of cookies, which makes user permission void in any case.[91]

2.1.5 Personalisation Algorithms: From Prediction to Determination

When it comes to social media companies' data practises it's also relevant to understand how they use that data. Aside from selling data, these companies make use of the data for various feature updates to their apps, services and to improve the personalisation algorithm.

There was a time when social media was still a novel experience, and Facebook had been newly introduced. At this time, the newsfeed feature was introduced. Posts from users' friends and pages that they had liked would appear on each of their individual feeds in chronological order. So, the post that was uploaded first would be seen first and only those posts would appear that the user had in a way subscribed to by following, liking or friending an account. However, personalisation algorithms changed this with the express purpose of getting users to stay online on the social media platform for longer; in a way that would encourage addiction. In some cases, this started out with restructuring how posts appeared on the feed. Instead of following a chronological order, posts on platforms such as Facebook and Instagram began to be displayed based on popularity. So, posts with more likes and engagement would appear first. In many cases, this meant that uploads by popular social media pages or accounts of personalities such as celebrities or influencers were pushed more than those of a user's personal friends.

This was experimented with to become more personalised so that each user's feed had content sorted according to their preferences, which even with minimal surveillance was simple to infer just based on what kind of posts users liked, disliked, commented on, shared or even skipped. More features were added to allow users to express their emotions

[91] Degeling et al., 2.

or reactions to content on social media, however, conversely these features meant greater surveillance as well. Facebook introduced a range of reactions, adding to the simple like and dislike feature, expressions of happiness, sadness, anger, surprise, compassion and love. Other features include tracking how users view videos, how long they watch it, or if they decide to quit it part of the way, at which point in the video do they quit or skip ahead, how many times they replay a video and more. This is especially integral to YouTube content metrics, but it has become more common since the popularity of the short-form video format which started from TikTok but is now a main feature on other platforms as well, such as Reels for Instagram and Facebook. It's also important to note that the popularity of video content now allows surveillance business models even more insight into individuals' private lives as it naturally carries more material to be datafied than a text or image post.

2.1.1.2 Social Media Led Tunnel Visioning

Aside from reorganising newsfeed updates, most social media platforms now have suggested content that peppers regular posts appearing on a user's feed with posts from accounts that they do not even follow. This includes sponsored posts or ads[92] that the user is forced to scroll past given the design of the app. Suggested content is meant to keep the user's feed running endlessly since, generally speaking, there are only so many people users can follow on social media who can only post so much content. However, like television channels adopted a model that allowed tv content to never sleep or run out, social media was able to do the same. The content discovery feature is a case in point, where social media platforms, in addition to the user's own feed, also have a discovery or explore page that is customised to each user with content from all over the platform. This is where the personalisation algorithm really works its charms as it utilises all the different data it has compiled from each users' activity on the particular social media platform, other associated platforms, apps, the internet, and their devices. That is not all,

[92] White and Boatwright. "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations."

social media can also gain insights from users' social media friends' online activity as well as family members' activity that can be monitored through devices connected on the same network. The algorithm uses insights from all this data to show users' the exact content that it deems they would likely engage with. Note, I use the word 'engage', not simply 'like', because social media companies have figured out patterns to appeal to users' range of emotions to keep them online. So, even content that would anger someone, like controversial posts which would prompt users to express their aggravation by commenting underneath posts drive engagement and are deliberately pushed forward by the algorithm. Ultimately, what we have is a stream of content that is being filtered by a computer algorithm which we do not fully understand or can predict for ourselves. This can lead to a number of problems, such as social media users being shown content that the algorithm pushes towards them based on their or their social media connections' past interactions with different content. So, users will mostly see the same type of content which generally aligns with their views and preferences, or that of their friends' and this can lead to a type of tunnel visioning in terms of content. The implications of this can mean that as social media increasingly comes to replace other sources of information, such as books, news publications, TV and healthy discourse in general, users are not being exposed to diverse viewpoints, whereby they can make informed opinions for themselves. By design, it is extremely difficult for users to wilfully search and look for different kinds of content and viewpoints on social media.

2.1.1.3 Selling Predicted Behaviours

This becomes even more of a problem when we consider another one of the data companies' business strategies, which Zuboff calls the 'behavioural futures markets.'[93] She explains, 'the stakes are high in this market frontier, where *unpredictable behaviour is the equivalent of lost revenue.'*[94] What this means is that social media companies and other surveillance businesses now have enough data to bet on user's future behaviours.

[93] Zuboff. *Age of surveillance capitalism*. 153.

[94] Zuboff. 153

This includes peddling targeted information or ads, such as pushing a notification about McDonalds' discount deal on the user's device when they are near a McDonalds' store, as determined by their geolocation. It has also opened up the market for predictive products such as AI assistants that are programmed to become better at predicting the user's needs, by learning their routine next and patterns. In this way, companies like Google and Meta are not just selling user data, but they also sell predicted, assured future behaviours that users can be prompted to execute through targeted digital cues. Such an equation between a user and a corporation already creates a power imbalance between the two. For the purposes of this paper, it is vital to consider the ramifications of what this much control and access to citizens in the hands of foreign agencies can be.

2.2 Emerging Social Media Threats

The above sections delved extensively, albeit still briefly, into the various aspects of the surveillance capitalism model and what it means for society, human behaviour, their right to privacy and security. In many ways, the threat it poses to a nation's human resource and the state's integrity is obvious. There is ample literature, including research, journalistic investigation and even court proceedings that prove social media companies' surveillance practices. Moreover, the fact that agencies such as the NSA make open use of these surveillance mechanisms is also well-documented from the Snowden case to Russia's alleged manipulation of the 2016 US elections. During the election campaign, posts sponsored by Russia which stated that Trump was endorsed as an election candidate by the Pope circulated on users' newsfeed without the sponsored tag which many ended up believing as factual news.[95] Facebook's advertisers include political entities, special interest groups, fake organisations and even organisations that seek to radicalise.[96] There is, as of yet, no mechanism in place to counter fake news or manipulative information on social media. This of course is not a localised problem, but the global nature of social

[95] White and Boatwright. "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations."

[96] White and Boatwright. "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations."

media does make it an international problem. As discussed in the previous chapter, the Snowden leaks uncovered that many government agencies were surveilling the data of citizens belonging to other nations, which included Pakistan. Engelhardt et al. state that foreign users become especially vulnerable to NSA's wiretaps under the 'one-end foreign rule'[97]. Social media user surveillance gives foreign companies and security agencies access to in-depth data of other countries' data with a breadth and depth that their own state institutions are not privy to. As we have seen, by applying a surveillance capitalism framework to the question of social media user surveillance and its threat to security, we know that the problem does not simply end at access to citizen data. When we say citizens, it includes sensitive persons, computer systems and devices that house sensitive information which are barely protected by Pakistan's existing policies. Internet and social media user surveillance open these systems up to even more vulnerability.

In terms of Pakistan's cyber security policy, the problem is not just lack of regulation but lack of awareness as well. Many vital concepts that are now being explored and adopted by other competent national policies such as the concept of 'data sovereignty' are missing from Pakistani policies. The problems that stem from a surveillance capitalism order are, just as in regular capitalism, exacerbated for countries like Pakistan, owing to inequalities. In this case, it is digital inequality, which means that Pakistan, owing to its low literacy rate and even lower digital literacy rate, lack of quality digital systems and effective policy and legal frameworks, ultimately makes its cyber space vulnerable. Taking realism as its theoretical framework, together with surveillance capitalism as the conceptual framework allows this research to frame the problem of social media user surveillance within the context of the data economy. It helps us not only define what surveillance through social media looks like, but also highlight the problems it poses—problems that continue to evolve under the current capitalist model. Ultimately, this allows us an understanding of cyber security threats that emerge from social media user surveillance

[97] Englehardt et al., "Cookies that give you away: The surveillance implications of web tracking," *In Proceedings of the 24th International Conference on World Wide Web,* 1: (2015). https://dl.acm.org/doi/pdf/10.1145/2736277.2741679.

that Pakistan as a youthful and developing nation, with much of its population on social media, is very much vulnerable to. It is only through developing an understanding of the nature and scope of the threats posed by social media surveillance that we can begin to devise solutions.

Conclusion

This chapter went into an explanation of the surveillance capitalism conceptual framework, linking it to the practice of social media user surveillance in order to better understand the dynamics of the economic model that sustains it. In doing so, we have tackled the first research question posited by this thesis, which sought to determine what are the cyber security threats that emerge from social media user surveillance. Applying the conceptual framework to the topic at hand allowed insight into the different ways in which user data is vulnerable to surveillance and theft. This also means that users themselves become vulnerable to manipulation by big data companies, including but not limited to, social media companies. Touching upon the privacy and security violations, ethical concerns, and still emerging challenges of social media user surveillance builds a solid argument for why Pakistan’s cyber security policy should consider it a cyber security threat that should be addressed in its policy.

The next chapter will critically analyse the privacy policies of Facebook and YouTube as a case study of two specific social media companies, to better understand how these companies collect and process user data. This will be followed by an analysis of existing cyber security policies and legal frameworks in Pakistan to determine the extent to which data protection is understood and implemented at the policy level.

Chapter 3

CRITICAL ANALYSIS OF EXISTING POLICIES

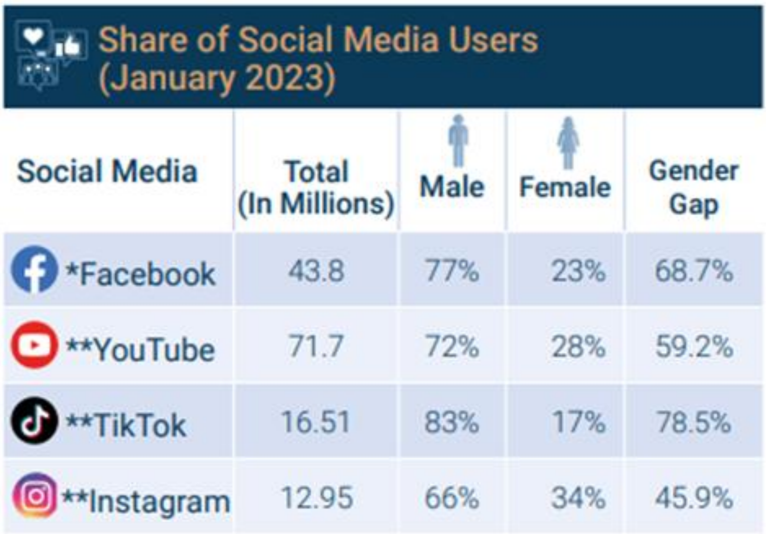
In this chapter, the privacy policies of Facebook (Meta) and YouTube (Google) will be studied along with secondary documents such as existing policy reviews, analyses and reports of the companies' policies, to get an overall understanding of how each platform engages with user data. A critical analysis of the selected social media companies' privacy and data collection policies will give insight into their social media surveillance practices, and thereby highlight the vulnerabilities that users and their data are exposed to when using such platforms. This, in turn, will help figure out what specific provisions are needed in terms of policies and regulatory frameworks.

This section will also go over Pakistani policies to understand what legal framework exists to ensure citizens' privacy and right to information in general, and then also analyse laws specifically related to data privacy. The main document, which would relate to the particular thesis of this research is the Personal Data Protection Bill 2023. A comparative analysis of the clauses in this bill that are directly related to data protection and social media with the privacy policies of Facebook and YouTube will help gauge how effective existing Pakistani policy is. This technique will show to what extent present data collection and regulation policies address social media user surveillance practices, and thereby, explore the way forward for improvements.

3.1 Why Facebook and YouTube?

The foremost reason for choosing the privacy policies of Facebook and YouTube as subjects for this study is that, as discussed in the previous chapter, each of their parent companies, Meta and Alphabet respectively, are not only among the biggest tech companies, but they also rank amidst the top ten global companies. This indicates that these two social media platforms, in particular, have the highest revenue generation, advancement in technology and widest global reach. All of which gives Facebook and YouTube, and by extension, Meta and Google, a competitive edge in terms of boasting the most advanced features. This includes the most progressive social media surveillance technology. Even in the legal realm, these companies have done the most towards developing rules and policies for social media data collection and user policy. Facebook is especially known for its recurring legal battles that has led to it revising its policies time and time again. Moreover, the influence these corporations enjoy means that they have ties with law-making organisations, even at the global level, which are susceptible to their strong lobbying.[98] Ultimately, these companies are among the pioneers of social media services and technology, so much so that they set the standard in the industry. Studying their practices and policies would give us a good idea of how user surveillance operates across the board, and what are the key challenges that any effective policy should be addressing to regulate online surveillance and data collection even beyond social media. It is also important to note that, as per the Pakistan Telecommunication Authority’s (PTA) statistics published 2023, Facebook and YouTube are the most used social media platforms in Pakistan with 43.8 million and 71.7 million users respectively (see **Figure 3.1**).

[98] Zuboff. *Age of surveillance capitalism*.



Share of Social Media Users
(January 2023)

Social Media	Total (In Millions)	Male	Female	Gender Gap
*Facebook	43.8	77%	23%	68.7%
**YouTube	71.7	72%	28%	59.2%
**TikTok	16.51	83%	17%	78.5%
**Instagram	12.95	66%	34%	45.9%

Figure 3.1: Number of Active Social Media Users by Platform in 2022 published by Pakistan Telecommunication Authority (PTA).[99]

3.2 Critical Analysis of Social Media Privacy Policies

As laid down in the research methodology section, the privacy policies of each Facebook and YouTube will be primarily analysed with respect to the following categories, i) what data each platform collects and how each does it, ii) how data is processed and who has access to it? iii) how data is stored and transferred and iv) what are their consent and transparency procedures? (See Table 1 for summarised results). The main sources for this analysis will be the publicly available online privacy policies uploaded by each platform. For Facebook, this falls under the Meta 'Privacy Centre' website[100] that couples together the policies for what it calls its products (Facebook, Instagram and other services—this excludes WhatsApp), as well as any specific policies for Facebook itself. For YouTube, there exists separate YouTube privacy guidelines[101] and user controls, and also a

[99] Pakistan Telecommunication Authority. *Annual Report 2023*.

[100] Meta. "Privacy Policy." Meta Privacy Centre, 27 December, 2023. https://www.facebook.com/privacy/policy/?section_id=0-WhatIsThePrivacy.

[101] Google, "Understanding the basics of privacy on YouTube apps." YouTube Help, accessed 1 June, 2024. https://support.google.com/youtube/answer/10364219?hl=en#zippy=%2C

highlighted section under the Google privacy and terms web page,[102] which provides an overarching privacy framework for its different services. This research will also consider any Google policies that seem relevant to YouTube data handling in general. Moreover, the analysis of policies will be supplemented with privacy reports published by the Common Sense Privacy Program, which independently evaluates platforms for child safety and privacy. These reports have audited both Facebook and YouTube's policies for adherence to recognised privacy laws and given it privacy ratings accordingly. Other secondary sources, such as relevant think pieces, and articles concerning these sites' data and privacy policies will also be referred to.

Table 3.1. A summary of Facebook and YouTube data policies

Categories	Facebook (Meta)	YouTube (Google)
Data collected	• Submitted information • User activity on Facebook and Meta products • Friends' activities on Meta products • User activity off Facebook • Through business partners, ad partners and various other third parties • Does not collect data of children under the age of 13	• Submitted information • User activity on YouTube and Google products, services, and devices • Metrics related to YouTube videos watched and uploaded • User activity off YouTube • Through business partners, ad partners and various other third parties • Collects data of children from YouTube Kids
Data processing and who can access it	• Data is processed through storing, sharing, analysing, profiling, reviewing, curating • It is used for personalisation, ads, research, security, and improvements	• Data is processed through storing, sharing, analysing, profiling, reviewing, curating • It is used for personalisation, ads, research, security, and improvements

[102] Google, "Privacy Policy." Google Privacy and Terms, accessed 1 June, 2024.https://policies.google.com/privacy?hl=en-US

	• Partners, service providers, integrated partners etc. • Government data requests including US national security requests—FISA can access foreign users' data	• Partners, service providers, integrated partners etc. • Government data requests including US national security requests, that request pen registering and wiretapping—FISA can access foreign users' data • Advertisers are restricted from misusing data, such as by way of having weak security or sharing PII with Google
Storing and transfer of data	• Data centres across the US, Europe and in Singapore • Transfer of data is subject to certain laws such as EU-US and Swiss-US Data Privacy Framework	• Data centres across the US, Europe, Middle East, South Africa, and East Asia • Transfer of data is subject to certain laws such as EU-US and Swiss-US Data Privacy Framework
Consent and transparency	• Users can download all available data • Choose to delete certain or all data • Change their ad preferences by editing a list of advertisers • Have limited choice over what data Facebook can use for showing ads • Policy supplemented with guiding illustrations and videos • Very expansive policy spread across numerous web pages, difficult to read	• Users can download all available data • Choose to delete certain or all data • Change their ad preferences by editing a list of advertisers • Have limited choice over what data Google can use for showing ads • Changing settings for YouTube or Google account still means data can be collected from various other sources • Concise and shorter policies that are easier to go through

3.2.1 What Data is Collected and How?

Facebook. Meta's privacy policy lists down that it collects data that users provide

Facebook when creating an account such as name, age, email, phone number. In addition, it also collects user-generated content (UGC) including posts, comments, and more. User activity such as reactions to posts, when the user is active on the platform, how much time they spend there, what they click on, etc is also collected. The same amount of information is also collected about the user's friends as well as followers on Facebook as data associated with the user's data profile. This means that the user's friends' activities on the platform and their preferences will not only be used to profile them as individual users, but it will also help Facebook ascribe certain characteristics to the main user. For example, if your friends like a certain post, Facebook can surmise that you might like that post too, and hence, push it onto your feed, and even show you ads related to pages or content your friends have liked. It also collects data related to how you interact with your friends and others on Facebook, including which of your friends you interact with the most and how you choose to do so. The policy also states that it collects information about the device the user is using Facebook on, such as its type, model, IP address and more. However, the policy explicitly mentions that despite concerns regarding Facebook listening in to users' speech or conversations, it does not access the device microphone except when it is actively used for a feature such as recording a video or audio message.[103] Nonetheless, the policy does not say all the features it needs to use the microphone for, and within device settings, when granting Facebook permission to use the device microphone, there are no conditions on how and when the app can use it. So, practically speaking there is no regulation or mechanism in place to prevent the social media site from accessing the microphone. The same can be said for other device features.

Lastly, the policy lists data gathered from their 'partners', which it states can include users' online as well as offline activity taken from other websites and apps they visit, any services they use like making purchases on other websites, online games they may play, etc. There is no official list of partners, but the policy describes them as, 'A person, business, organisation or body using or integrating our Products to advertise, market or

[103] Meta. "Privacy Policy." Meta Privacy Centre, 27 December, 2023. https://www.facebook.com/privacy/dialog/is-facebook-listening-to-my-conversation/

support their products and services.'[104] Understandably, this would mean Facebook has access to a vast list of partners. Some of these partners that are collecting data from user activity and sharing it with Facebook can be reviewed by users through their privacy settings. Doing so would reveal that almost every website that you have visited and even those you may have never visited, are able to share the data they have collected about you, such as user activity, cookies etc. with Facebook. A recent study conducted found that for the 709 participants, an average of 2,230 different companies shared their data with Facebook.[105]

It is also crucial to note that Facebook also collects data of users who do not have an account on its social media platform, either by way of when they visit the Facebook website and interact with it in any way, or through how they interact with any of its partners' websites and services. Similarly, with regards to location, the policy states that even if users choose not to share their location with Facebook, it is able to access their location through other sources such as through data collected by its, metadata from photos which users have given the platform access to, and by estimating their general location through their IP addresses. It is pertinent to note that data collected by Facebook per user is taken together with data from other Meta products such as Instagram and Messenger. Access to multiple social media profiles of the same user can help Meta triangulate users' information and account for missing data that might not be available on Facebook alone, and thus allows it to have greater access to the personal details, daily activities and characteristics of each user.

For certain sensitive information, such as a user's religious and political beliefs, trade union memberships, and ethnicity, the policy may assign special protection to it depending on local law of the user's jurisdiction. Additionally, Facebook's policy does

[104] Meta. "Privacy Policy." https://www.facebook.com/privacy/policy?annotations[0]=Definition-Partner.

[105] Marti, Don, Fengyang Lin, Matthew Schwartz and Ginny Fahs. *Who Shares Your Information With Facebook? Sampling the Surveillance Economy in 2023.* New York: Consumer Reports, 2023. https://innovation.consumerreports.org/wp-content/uploads/2024/01/CR_Who-Shares-Your-Information-With-Facebook.pdf

not allow children under the age of 13 to own accounts on its platform as part of its safety procedures. If it comes to know that an account is being run by a child, it deletes that account, and all data associated with it.[106]

It is imperative to note that with every detail that the privacy policy admittedly reveals, there is more that it may not have chosen to explicitly state. With words like 'such as' and 'like' being used before the policy gives two or three examples of what data it collects and how it collects it, it's impossible to know all of what Facebook collects, or have an understanding of all its surveillance methods. Although, one way individual users can see all the data Facebook has on them is by requesting to download all their information. However, dubious language in the policy means that despite the attempt at an easy-to-read, detailed policy, it still lacks transparency.

YouTube. Data collected directly from YouTube includes metrics related to its video content such as users' watch history, engagement with videos like watch time, likes, dislikes, comments as well as content created and uploaded by users. An interesting feature of YouTube is its video engagement analysis, through which it studies metrics such as sections of a video that are most watched, replayed, skipped, and more. While Facebook also monitors similar metrics, YouTube relies on it for its main content—its videos.

Essentially, YouTube collects almost all the same data that Facebook does, including ad related data and data from partners. However, it's important to remember that YouTube falls under Google's products and Google has access to a much wider range of data sources through services such as the world's largest search engine, Workspace, Maps, Cloud, and many others. This clearly indicates that for every user, YouTube likely has access to more data and different types of data. The Google privacy policy lists that it

[106] Meta. "Safety Resources for Parents." Facebook Help Centre, accessed June 1, 2024, https://www.facebook.com/help/1079477105456277.

collects information such as all details related to an android user's app downloads through its Google Play service, more precise data (in comparison to Facebook) of android users' devices like crash reports and network connection status, and all activity on Google Chrome browser—which basically includes every single activity of a Chrome user on the internet—and other Google services such as emails through Gmail. Moreover, the policy states that it estimates user location through GPS, IP addresses, nearby cell-towers, blue-tooth enabled devices and 'sensor data from your device'[107] among other features. While the separate YouTube privacy settings page says that it only uses the general location, which is larger than 1 sq mi, and has at least 1,000 users within its range,[108] the Google policy, which also applies to YouTube, clearly has access to the pinpoint location of users, as is evident through the accuracy of its Google Maps product. Additionally, use of sensor data which the policy says includes the phone's built-in accelerometer, barometer, magnetometer, and gyroscope, suggests that not only Google, but even various apps on a device can have access to device features such as the microphone and motion sensors, which can collectively gather large amounts of data of users' offline activities.[109] In fact, Google's policy already mentions that it records users' audio inputs and collects information about their voice for use in services such as the voice-operated Google Assistant. Again, like with Facebook, there is no way to tell which particular service features require the use of microphone and other device features, so it is impossible to know exactly which and when these companies are surveilling users. Although the policy states that Google Assistant remains in standby mode until prompted by the activation command, 'Hey Google', it does not record any speech aside from the direct input to the Assistant and a few seconds before the command was given, it is clear that Google does have access to the user's device microphone at all times. The previous chapter already noted how a smart TV using the Android operating system recorded household conversations containing private information from individuals who had spoken in the

[107] Google, "Privacy Policy." https://policies.google.com/privacy?hl=en-US.
[108] Google. "Understanding the basics of privacy on YouTube apps." https://support.google.com/youtube/answer/10364219?hl=en#zippy=%2C
[109] Kröger and Raschke. "Is my phone listening in? On the feasibility and detectability of mobile eavesdropping." 111.

vicinity of the device.[110] Moreover, a research study found that Android devices receive around 40 to 90 hourly requests for data related to the device's use and user from Google.[111]

It is worth noting that even if Google itself is cautious of user privacy when making use of built-in device features and the data that is collected from it, there are many apps and websites, including those on Google Play, as well as the Apple store that have failed to pass privacy screening tests.[112] These apps and websites can establish unauthorised access to Google's devices and features to collect user data. Data collected from the myriad of Google services and devices is relevant to YouTube's privacy policy because this data is supplemental to data collected directly by YouTube. Moreover, the different Google services and features aid Google in collecting more data when a user is using YouTube. This collective data then shapes the user's experience of using YouTube, which then generates additional data for use and analysis by Google, thereby creating an almost inexhaustible loop of data collection. This goes on to show how owning a massive portfolio of data sources gives a multibillion tech corporation like Google almost endless access to data of users around the world.

In terms of its policy for children's data, YouTube also requires that users must be above the age of 12 to make an account. However, it does allow children use of its services with certain means of parental supervision enabled. YouTube Kids for instance gives parents control over how children use the service and what content they watch. Data of children, including voluntarily submitted personal information, data related to the user's device, metadata, and more, is collected as part of YouTube Kids terms and service. Certain data has more protection, for instance, voice data collected from children when they use YouTube Kids is deleted after use. Generally speaking, however, the way in which children's data is processed and used is mostly covered by the same Google privacy

[110] Zuboff. Age of surveillance capitalism.
[111] Kröger and Raschke. 111.
[112] Kröger and Raschke. 113.

policy that applies to all other user data.[113]

3.2.2 How is Data Processed and Who Can Access It?

Facebook. The main ways in which Facebook processes the data collected is by storing, sharing, analysing, profiling and reviewing it. Most of the ways that Facebook processes data have been discussed in the previous chapter under how companies generally process user data, particularly how data is sorted, analysed and profiled. In terms of what the data is used for, the Meta policy states that user data is stored and accessed for personalisation, showing ads, performing analytics, sharing analytics and insights with businesses, advertisers and other partners, updating the platform's features, research and development, and maintaining security.

The policy says that 'in some cases', particularly for feature optimisation and advertising, Facebook uses anonymised, aggregate lists that have data stored without the users' names. For advertising in particular, Facebook makes lists of users who match the target audience of its ad clients and allows businesses to have access to and advertise to those users that are on the list. This means that if a company, A, has a product it wants to advertise to female users, ranging from the ages of 18 to 40, living in Pakistan, Facebook will accordingly show company A's advertisement to those who fall into its target audience. However, it is pertinent to mention here that aside from businesses that bid for ad space on Facebook, it has other partners such as integrated partners and essential service providers. For instance, financial transaction service providers which allow transactions to take place on Facebook. Such partners are third parties which have access to various data of Facebook users, including their financial data. The vast number of partners that Facebook has including various services, businesses, websites, and other apps, each with different levels of access to its user data, essentially indicates that there is no precise way to know what data and how much data of each user is being shared.

[113] Google. "Terms of Service". YouTube Kids, accessed 1 June, 2024. https://kids.youtube.com/t/privacynotice.

Moreover, even though Meta's policy states that partners and third parties who have access to its user data must follow certain rules pertaining to what they can do with the data, there is no well-enforced comprehensive regulation that limits these parties to sell that data forward. While Facebook claims it does not directly 'sell' user data to anyone, it is evident that through various agreements and arrangements, the social media company is allowing an unknowable number of entities access to user data.

Highly relevant to this study, is the fact that such entities include the government of different states, law enforcement, legal bodies and in particular, the intelligence organisations of the US. The Meta policy specifically mentions that in addition to various other laws of the US, the Foreign Intelligence Surveillance Act (FISA) compels it to submit the data of any user, belonging to any region.[114] Moreover, it states that it is obligated to respond to US national security requests, including emergency disclosures. The data that these state entities can request are pulled from beyond Meta products, so not just Facebook, Instagram, or Messenger, but WhatsApp as well. According to disclosed statistics, Meta reports that worldwide, just between the period of June 2023 to December 2023, in total, 301,553 data requests were made by governments, which together requested the data of 528,232 users.[115] From these, the US alone had made 73,390 requests, of which 4,199 were emergency disclosure requests.[116] Pakistan made 1,614 requests, with 58 of them being emergency disclosures, for access to the data of 1,942 users.[117] It is important to note here, that for the US at least, these numbers include foreign nationals whose data it can access because of its own laws. The same cannot be said for Pakistan, since countries such as the US, China and the EU have laws in place to prevent export of user data. which means from a national security standpoint, that certain countries, like the US have an upper hand when it comes to having access to citizens and their information through social media and use of internet than do other countries. This

[114] Meta. "Government Requests for User Data." Transparency Center, accessed 1 June, 2024. https://transparency.meta.com/reports/government-data-requests/further-asked-questions.

[115] Meta. "Government Requests for User Data." https://transparency.meta.com/reports/government-data-requests/.

[116] Meta. https://transparency.meta.com/reports/government-data-requests/country/US/.

[117] Meta. https://transparency.meta.com/reports/government-data-requests/country/PK/.

is also evident from the statistics which show that while the US has had 88.54%[118] of its requests for data approved by Meta, in comparison, Pakistan has had 75.46% requests approved.[119] This reflects the difference in access to data between the US and Pakistan.

YouTube. Data collected by YouTube is processed and used in much of the same ways as Facebook uses it. For instance, the data is used to personalise user feed on the video-sharing site, optimise features, show relevant ads, etc. It is important to note that YouTube, unlike Facebook, but more like Instagram, relies on its interaction with paid creators. YouTube's main content mainly comes from users who upload videos for monetary return. Facebook has a monetisation framework as well, but it is not as dependent upon it as YouTube is, hence it is not as well developed and utilised as YouTube's monetisation process. As part of its interaction with content creators, YouTube uses extensive analytics of videos and user engagement to improve or redefine its algorithm to gain the highest number of views. It also shares some of its analytics with creators so they can learn to create content that should be able to garner more engagement. Additionally, the Google privacy policy outlines that data is shared with affiliates and 'trusted' business partners for external data processing[120], and to state or enforcement agencies for legal reasons. Similar to Facebook, Google has also published statistics about government data requests. Globally, from the period of January 2023 to June 2023, it received 211,201 requests for the data of a total of 436,326 users.[121] In the same time period, the US made 81,271 data requests, which are separate from its national security requests. Interestingly, Google statistics are broken down into several categories for US data requests, including requests for pen registering and wiretapping, and this is just for requests unrelated to national security.[122] Meanwhile, Pakistan placed 17 requests for the

[118] Meta. https://transparency.meta.com/reports/government-data-requests/country/US/.

[119] Meta. https://transparency.meta.com/reports/government-data-requests/country/PK/.

[120] Google. "Privacy Policy." https://policies.google.com/privacy?hl=en-US#infosharing.

[121] Google. "Global requests for user information." Google Transparency Report, accessed 1 June, 2024. https://transparencyreport.google.com/user-data/overview?hl=en_US.

[122] Google. "Global requests for user information." https://transparencyreport.google.com/user-data/overview?hl=en_US&user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period

disclosure of 86 users' information.[123] The considerable difference between the requests Pakistan made from Facebook versus Google may reflect the Pakistani policies focus on monitoring social media users in violation of its content and media laws. Additionally, it might also have to do with the fact that its approval rate of requests to Google is only 18%[124], which is much less than that of Facebook's for Pakistan.

While Facebook, in its publicly available advertising standard policy focuses on the kind of data that is permissible on its platform, what stands out about Google's policy is that it makes publicly available the kind of data privacy rules that are enforced against advertisers. It lists some examples of what it does not allow advertisers to do with user data such as, failing to implement adequate security for each type of data, sharing personally identifiable information (PII) with Google—this does not apply to selected partners, misusing personal information and setting unauthorised cookies on a Google domain.[125] The privacy policy also clarifies that Google itself does not share identifiable data with advertisers. However, despite both Meta and Google claiming this, bear in mind that the amount of data per user that is shared with advertisers and other third parties can allow them to figure out a user's identity through the analysis of and inference from the collective data that they may have amassed from various sources.

3.2.3 Where is Data Stored and How is It Transferred?

Facebook. According to Meta policy, user data is stored across the globe in its data centres and is also transferred through worldwide networks to its partners and third parties located around the world, which it states is essential to its functioning as a social media platform. It further mentions that all data handling is subject to international law on data

[123] Google. "Global requests for user information." https://transparencyreport.google.com/user-data/overview?hl=en_US&user_requests_report_period=series:requests,accounts;authority:PK;time:&lu=user_requests_report_period

[124] Google. https://transparencyreport.google.com/user-data/overview?hl=en_US&user_requests_report_period=series:requests,accounts;authority:PK;time:&lu=user_requests_report_period

[125] Google. "Data Collection and Use." Advertising Policies Help, accessed 2 June, 2021. https://support.google.com/adspolicy/answer/6020956?hl=en#zippy=%2Ctroubleshooter-unacceptable-information-sharing

privacy. While the UN General Assembly did adopt the Right to Privacy in the Digital Age resolution, its draft for a data privacy framework is still being worked upon. So far, only the GDPR is seen as the most influential standard in data privacy laws worldwide. Additionally, where it is mandated to, Facebook is obligated to comply with local laws as well. For instance, the 2023 EU-US Data Privacy Framework, specifies rights and protective conditions for the transfer of EU users' data to the US, including laws for whose data can be transferred. Russia has threatened to ban Facebook over demands to localise its users' data within its borders. However, this did not materialise, and instead Facebook as well as YouTube, and other social media platforms have banned ads in Russia, and ads from Russian creators due to the ongoing conflict with Ukraine.[126] Currently, Meta lists that it has its largest cluster of data centres in the US, alongside, a few across the EU, and one large centre in Singapore.[127] From a national security perspective, it is important to know where citizens' data is stored and how well it is protected by the company in-charge of it, in this case, Meta, and also by state law on data regulations of the country where the data is stored. It is also important to note, all user data collected by Facebook is owned by Meta,[128] so in the case that the company were to be sold, most of the data will be handed over to the new owner, which will have its own policies.

YouTube. According to Google policy regarding storage of data, its website states:

> Rather than storing each user's data on a single machine or set of machines, we distribute all data — including our own — across many computers in different locations. We then chunk and replicate the data over multiple systems to avoid a single point of failure. We name these data chunks randomly, as an extra measure of security, making them unreadable to the human eye.[129]

[126] Meta. "About Meta Advertising Standards." Business Help Centre, accessed 1 June, 2024. https://www.facebook.com/business/help/488043719226449?id=434838534925385

[127] Meta, "Meta Data Centers." Data Centers at Meta, February 23, 2024, https://datacenters.atmeta.com/.

[128] Su and Tang, "Data Sovereignty and Platform Neutrality," 66.

[129] Google. "Data and Security." Google Data Center, accessed 2 June, 2024. https://www.google.com/about/datacenters/data-security.

Similar to Facebook, Google has its data centres clustered in the US, the EU, and a few in South America and East Asia. As for its Cloud locations, they are stored in centres located in South Africa, Qatar, Saudi Arabia and Germany, and it is continuing expansion in other countries as well.[130] It is no surprise that given that Google generates and collects a much larger amount of data, it has a greater number of data centres that are spread across many different regions.[131] As for data transfers, Google lists the same legal frameworks as Facebook, the EU-US and the Swiss-US Data Privacy Frameworks, in addition to clauses by the EU which mandate special protections for data transfer from European Economic Areas (EEA) to other countries.

3.2.4 Content and Transparency Procedures

Facebook. When making an account on Facebook, the website links you to three separate web pages including the terms page, privacy policy and cookies policy. Each of the links takes the user to a plethora of interlinked pages and resources that would require a great amount of time and attention from each user to go through. Moreover, the extensive amounts of links going from one page to another, and hyperlinks embedded within each text is extremely difficult to keep up with for users. A number of studies done on the subject indicate that even when users attempt to read privacy policies, most fail to fully understand it.[132] Although, it is apparent that Meta has attempted to make the policies more accessible through the use of colourful illustrations and explanatory videos (see Figure 3.2). The dilemma remains that if information is provided in a concise manner for the average user's ease, then the policy may not be able to disclose each and every detail with regards what data it collects and how it is used. This is evident in the lack of an

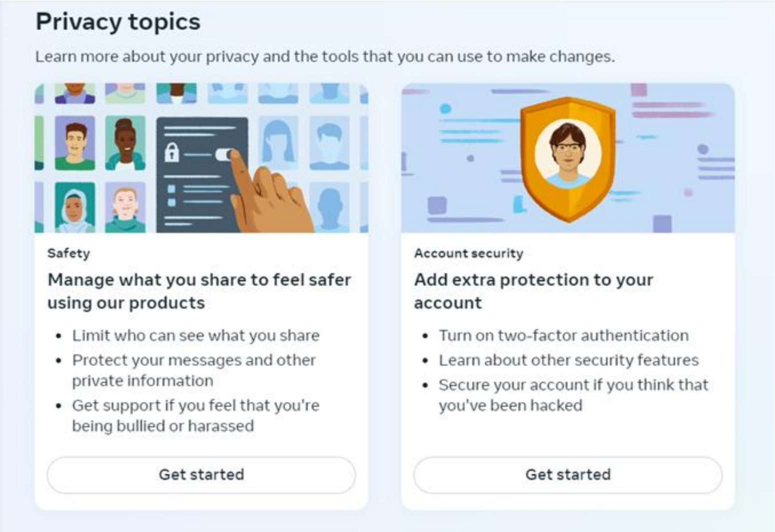
[130] Google. "Discover Our Data Center Locations." Google Data Center, accessed 2 June, 2024. https://www.google.com/about/datacenters/locations/?hl=en_US.

[131] Google. "Cloud Locations." Google Cloud, accessed 2 June, 2024. https://cloud.google.com/about/locations.

[132] Ibdah, Duha, Nada Lachtar, Satya Meenakshi Raparthi, and Anys Bacha. ""Why Should I Read the Privacy Policy, I Just Need the Service": A Study on Attitudes and Perceptions Toward Privacy Policies." *IEEE access* 9 (November 2021): 166465-166487. https://ieeexplore.ieee.org/abstract/document/9624976

exhaustive list of what data Facebook collects, among other things. Moreover, with how fast digital platforms and devices keep evolving, so do their policies, and social media sites like Facebook constantly keep changing their user-interaction designs which can be difficult to keep up with. [133]

As for privacy settings, Facebook's website provides a relatively easy-to-use means to review account settings, again supplemented with illustrations (see **Figure 3.2**), explanation cards and links to policy pages.



Privacy topics

Learn more about your privacy and the tools that you can use to make changes.

Safety

Manage what you share to feel safer using our products

- Limit who can see what you share
- Protect your messages and other private information
- Get support if you feel that you're being bullied or harassed

Get started

Account security

Add extra protection to your account

- Turn on two-factor authentication
- Learn about other security features
- Secure your account if you think that you've been hacked

Get started

Figure 3.2: Screenshot from Meta's Privacy Centre website showing its friendly UI design.[134]

Essentially, the Meta policy states that users can have access to all data that the social media company has on them. They can download and review this data, and request to delete any part or the whole of it, aside from certain data that is essential to using its services. Users can choose to opt out of targeted ads entirely or tailor their ad preferences by accessing the list of advertisers that have the users' information and manually

[133] Wong. "Smartphone location-based services in social, mobile, and surveillance practices of everyday life." https://www.lse.ac.uk/media-and-communications/assets/documents/research/msc-dissertations/2013/96-Wong.pdf.

[134] Meta. "Privacy topics." Meta Accounts Centre, accessed 2 June 2024. https://accountscenter.facebook.com/ads/

removing the advertisers they do not wish to see ads from. However, it is relevant to bear in mind that removing advertisers from Facebook does not affect the data they have of the user since according to the policy, their data is sourced from activity outside of Facebook. Users can also see which ad categories have been assigned to them, a long list based on each user's preferences.[135] For instance, in the researcher's own case, the list seems to comprise of general topics such as 'fun', 'party', 'food', to specific ones such as 'Islamabad', 'college and graduate education', 'Asian pasta', and for some reason, 'cash on delivery'. For any category on the list, users can choose to 'see less' of it. Additionally, as part of its 'Privacy Checkup' feature, Facebook guides users through their privacy settings, allowing them to customise their accounts' settings by choosing how their profile appears to other Facebook users, strengthen their account security and review which apps and websites are associated with their Facebook account. Removing these apps will prevent them from accessing the users' Facebook data. The Privacy Checkup[136] feature also allows users to choose which data can be used to show ads to them. However, this list appears to be very limited with only options such as the users' relationship status, employer, job title and education. It is worth mentioning that one of the challenges of Facebook's privacy settings is that it is widespread over various web pages and links. While some settings are found in the Meta privacy centre and accounts centre, others require you to directly interact with the Facebook website. Therefore, it is hard to judge exactly how much control users have over their privacy settings.

Facebook's 'Transparency Centre' is yet another feature that aims to educate users and businesses on its use of data as well as its role in security, governance, enforcement, and more. This is where it mentions its policy for government data requests, and states that no data is transferred without the explicit consent of users, especially with regards to sensitive information. However, both Meta and Google policies also state that if a country's data request especially prohibits them from informing users of data requests,

[135] Meta. "Ad preferences." Meta Accounts Centre, accessed 1 June, 2024. https://accountscenter.facebook.com/ads/.

[136] Facebook. "Privacy Checkup." Facebook, accessed 2 June 2024. https://www.facebook.com/privacy/checkup/.

then they are obligated to disclose the required data without consent.

YouTube. When a user creates an account on YouTube, they are prompted to create a google account, and accordingly it presents them with Google's privacy policy and terms that users must agree to. Google's policies, in comparison to Facebook, are more concise and streamlined. However, this is no indication of whether the policies are transparent and convey all information to the user. In terms of user privacy settings, YouTube has a dedicated page titled 'Your data in YouTube' where users can find options to opt out of saving their location history, watch history, search history, YouTube voice searches—interestingly, a category separate from general searches—web and app activity to their Google accounts.[137] While choosing not to save this information would mean that the user's YouTube suggestions and ads will not be personalised according to this particular data, it is unclear whether it also means that Google will no longer collect this data for its own database. YouTube offers a wider range of privacy control options for users who upload videos. Additionally, privacy settings for YouTube Kids are separate.

Only the limited types of data listed above can be controlled by users. Moreover, as discussed above, YouTube, like all other Google products and services, do not collect data from a singular source. So even if a user were to turn off their location history from being saved through YouTube, it does not mean that the actual data collector and processor, Google, will no longer have access to their location history. Therefore, users will have to turn to the privacy settings to Google's 'Privacy Center' and go through each of its different options for complete privacy control. Moreover, even if users change their settings through both YouTube's privacy controls and Google's Privacy Center, there are still other ways such as the use of Android devices with apps like Google Maps and Google Drive through which Google may still be able to collect user data. Going through each product and service's individual settings would prove to be a tedious and extremely

[137] Google, "Browse or delete your YouTube activity, and discover how your data makes YouTube and other Google services work better for you," Your data in YouTube, accessed 3 June, 2024. https://myaccount.google.com/u/0/yourdata/youtube?hl=en&pli=1

difficult task. Additionally, despite there being privacy controls, secondary sources including scientific studies show that all major social media companies and browsers lack transparency.[138] This means that when it comes to the different types and amount of data Moreover, even if users change their settings through collected, existing privacy settings are not exhaustive. It is also not provable that these companies stop collecting data even when consent is withdrawn.

3.2.4.1 Privacy Standard Ratings

To supplement the analysis, the research referred to Common Sense Privacy Program's review and rating of each of the privacy policies. This will give a better idea of the social media sites' actual adherence to privacy standards.

The review gives Facebook's privacy policy an overall score of 60% alongside a 'warning' label. While the policy scored high for protecting data from third parties and allowing users' the right to control their privacy settings, it scored low for all other categories, including protecting personal information, preventing unauthorised access, protecting children's data and preventing sale of data.[139] The YouTube policy gets a slightly better score of 77%, which also falls under the report's 'warning' zone. It generally scores considerably higher than Facebook on all categories. It scores highest in preventing unauthorised access and protecting data from third parties, while scoring in the 60-70 range for protecting personal information in general, protecting children's data, preventing sale of data, and preventing exploitation of users' decision-making process.[140]

[138] Kröger and Raschke, "Is my phone listening in? On the feasibility and detectability of mobile eavesdropping," 102-120.

[139] Common Sense Privacy Program. *Standard Privacy Report for Facebook.* Common Sense Media, 2022. https://privacy.commonsense.org/privacy-report/Facebook.

[140] Common Sense Privacy Program. *Standard Privacy Report for YouTube.* Common Sense Media, 2022. https://privacy.commonsense.org/privacy-report/YouTube.

3.3 Data Privacy Policy and Law in Pakistan

Article 14(1) of the Constitution of Pakistan declares the fundamental right to privacy for every citizen by stating that ‘dignity of man and, subject to law, the privacy of home, shall be inviolable.’[141] While this article only explicitly mentions the privacy of the home, Anwar et al., point out that in many cases, the Superior Courts have taken this to mean a general right to privacy.[142] Moreover, findings of the study so far clearly indicate how social media user surveillance encroaches upon the privacy of the home, as well as the dignity of man. Additionally, Article 19(A) relates to the right to information, as it states that ‘all citizens shall have the right to access information in all matters of public importance subject to reasonable restrictions by law.’[143] Thus, it becomes clear that protection from all kinds of surveillance, including social media user surveillance; and invasion of privacy, as well as the right to privacy of personal information and data, are all constitutionally guaranteed to each citizen.

The right to privacy has further been reinforced by several other laws passed in Pakistan. One such law is the federal law of Right of Access to Information Act, 2017, which stipulates that certain data which could potentially invade an individual’s privacy cannot be disclosed unless he requests it himself.[144]Each province has a comparable law that sets provisions for the right to information.

Laws that specifically relate to digital data can largely be traced to the COVID-19 era when widespread state surveillance of citizens had become integral to monitoring the spread of infection. For instance, the Punjab Infectious Diseases and Control Ordinance (2020) states that the data of infected individuals will remain confidential and only be

[141] Anwar et al., "Cyber Surveillance and Big Data-Pakistan's Legal Framework and Need for Safeguards." 37.
[142] Anwar et al. 37.
[143] Anwar et al. 37.
[144] Anwar et al. 38.

released to relevant persons like medical practitioners.[145] Khyber Pakhtunkhwa has a similar law related to epidemic control, but it is the Khyber Pakhtunkhwa Public Health (Surveillance and Response) Act 2017, which lays out direct provisions for surveillance by ensuring the confidentiality of personal health information and citizen data.[146] These laws, and others like this demonstrate that health-related data are legally considered private information in Pakistan, which means that such data being accessed by social media companies compromises the rights of Pakistani citizens.

3.3.1 Data Protection in Policy

To understand where Pakistan stands in terms of cyber surveillance and digital data, it makes sense to begin at the policy level. The main policies that contain guidelines for data privacy are the National Cyber Security Policy 2021 and the National Security Policy 2022. Given its scope, the latter policy briefly mentions the threat to citizens and the government from data theft. It especially identifies the critical requirement ensuring the security of privileged information, and hence, the need for developing secure local networks and devices that would allow protected and uninterrupted access to essential digital services.[147] Moreover, the policy lists data security among its policy objectives for information and cyber security. The existing National Cyber Security Policy 2021 recognises the lack of data governance in Pakistan, and acknowledges the need for data sovereignty when it states that:

> Countries face the threat of data colonization whereby data is managed, controlled, and processed out of the legal jurisdiction of the country and there is limited or no bilateral agreement among the stakeholders in this regard. Threat actors are liable to pollute the information domain and citizen data may be sold to third parties without due consent or validation… Weak governance of data, poor data quality, and absence of data stewardship

[145] Anwar et al. 43.

[146] Anwar et al. 44.

[147] National Security Division. *National Security Policy 2022.* Islamabad: National Security Division, 2022: 26. https://dnd.com.pk/wp-content/uploads/2022/01/National-Security-Policy-2022-2026.pdf.

> generate unreliable information resources and poses a threat to Cyber Security.[148]

This shows that current cyber security policy understands the link between lack of data governance and the threat to cyber security. The policy in its scope states that it envisions to secure the entire cyberspace of Pakistan, which includes protecting its digital assets including data that is processed, managed, stored and transmitted in the public and private sector. Moreover, it makes several mentions for the need of protecting citizen's online data privacy in its principles and as a policy objective. To achieve these objectives, it calls for relevant stakeholders to allocate the means necessary for data protection. It also directs stakeholders to come up with a Data Protection Framework, but specifically one aimed at securing government information systems and infrastructure, and not for citizen data in general. The policy also brings attention to the need for awareness about data protection and a national awareness programme. Data literacy and knowledge of protecting data and privacy rights is imperative as users are responsible for the security of their own data to a considerable extent.

Overall, the cyber security policy, while acknowledging the need for data protection both within local systems, and when interacting with international ones, still lacks a specialised understanding of the actual threats that data is vulnerable to. The policy makes no mention of surveillance, even as broadly as general internet surveillance. Its objectives and actionable clauses are generic statements which simply state that data needs to be protected. It is clear that as a singular national cyber security policy document, the 2021 policy cannot on its own sufficiently provide appropriate guidelines for social media regulation. There needs to be more work on drafting policy specifically aimed at data protection, and separate ones for social media regulation. The EU's GDPR is the most robust framework for data protection, however, it is still working on

[148] Ministry of Information Technology and Telecommunication. *National Cyber Security Policy 2021.* 4.

drafting an adequate social media regulation policy. This goes to show that, specialised policies that specifically aim to regulate social media's use of data are necessary to tackle vulnerabilities and threats that emerge from it. Even in terms of legislation, so far, Pakistan has only presented the final draft legislation of the Data Personal Protection Bill 2023.

3.3.2 The Personal Data Protection Bill, 2023

The final draft of the Personal Data Protection Bill that was made available in July 2023 legislates regulations for data controllers and processors. This includes any entity, including the government, which collects data, processes it in any way and has the capacity to disclose it. This definition technically includes all government institutions, educational institutions, small and large businesses, online retailers, apps, social media companies and others. While the bill is a monumental step towards data protection as it is the first to lay down rules for how citizens' data as well as critical data can be handled, it helps bearing in mind that one piece of legislation cannot adequately suffice for all the different kinds of entities that control or process data.

Some highlights of the bill are that it mandates the formation of a National Commission for Personal Data Protection, it requires all data controllers and processors to be registered with the Commission, it requires that major data controllers and processors appoint data protection officers, and it sets down consent laws for data subjects that data handlers must abide by, including separate provisions for children's data and parental consent. The bill gives data subjects certain rights, such as right to data access, right to erasure, right to nominate etc.[149] In terms of national security, the bill has an entire section dedicated to laws that enable the state to request access to essential data when it is in the national interest. Additionally, the bill stipulates that 'critical personal data',

[149] Ministry of Information Technology and Telecommunication. *Personal Data Protection Bill, 2023.* Islamabad: MoITT, 2023. https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf

which it does not clearly define, should be processed in servers or digital infrastructure within Pakistan.[150]

3.3.2.1 Critique of the Bill

Firstly, as mentioned above, this is not a bill specific to social media, but it does apply to social media companies as the only legislation for data controllers and processors. However, it is quite evident that the provisions within this bill are hardly adequate for the large number of complex challenges that emerge from social media user surveillance and data collection. The bill's main focus appears to be enforcing rules for all data that is being collected and processed. It does not, at all, provide any regulations for what kinds of data is allowed to be collected by which entities, and through what means. As we have so far established in this research, social media surveillance extends anywhere from collecting voluntarily submitted data to accessing users' devices in real time to directly surveil them. Although, the regulation of surveillance methods for data collection should fall within the outlined scope[151] of the bill, it does not seem to have covered this at all. It does however state that data collected should be justified according to the purposes that it will be used for and will only be processed so far as is adequate to serve these purposes. This is a welcome provision as it appropriately limits data collection and processing. However, more specifications for the different types of data processing entities are needed to allow proper enforcement of this law. Additionally, the bill's stipulations for consent mechanisms are also a right step in the direction of securing data and privacy. However, in certain instances, as the Digital Rights Foundation's (DRF) analysis of the bill points out, the way in which some clauses of the bill are worded, they run the risk of overriding consent requirements in certain cases.[152] This is particularly the case with clauses pertaining to the government's

[150] Ministry of Information Technology and Telecommunication. *Personal Data Protection Bill, 2023.* 29.

[151] Ministry of Information Technology and Telecommunication. *Personal Data Protection Bill, 2023.* 11.

[152] Digital Rights Foundation. *Analysis: Personal Data Protection Bill 2023.* Islamabad: DRF, 2023. https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf

right to access data when it is a matter of ‘legislative interest’, national security, and for other reasons. Media rights advocates have also criticised the bill for lacking accountability measures for the government and allowing the state unrestricted access to user data. They argue that the federal nature of the commission would lead to a conflict of interest, instead independent actors are needed to ensure strong protective measures.

The DRF, and other experts especially note the impracticality of demanding that critical data be processed locally. This particular provision in the bill, essentially requires data localisation of certain data. However, for social media companies and others providing international online services, data localisation proves a challenge since data is stored in different regions, and it needs to be transferred to various parts of the world for essential processing and services. Moreover, advocates also noted that Pakistan does not have the capacity for hosting its own large-scale servers and data centres, either technologically or in terms of power.[153]

The section of the bill related to transfer of personal data outside Pakistan lays down certain essential provisions as it restricts the transfer of critical data, preconditions the transfer of data on the data subject’s consent and only allows transfer to those areas which have adequate data policies. Technically speaking, this provision should counter the US FISA law, which can gain access to the data of any citizen without consent if it wishes to do so. However, there are sections in the bill that are contradictory to its own stipulations. For instance, the exemptions section removes the need for consent in the case of ‘research and collection of statistics.’ There are many ways in which this and other broad exemptions can be misused for data collection and processing, thereby rendering any consent mechanisms moot.[154] Other critiques of the bill noted the lack of contextualisation to Pakistan, with no specific provisions for the rights of women and their private data. Some noted that the draft was heavily informed by the UNESCO data

[153] Media Matters for Democracy. “Data Protection and Online Safety Laws' Impact on Media & Digital Freedoms in Pakistan.” July 31, 2023, legal analysis, 58:40, https://www.youtube.com/watch?v=0wn7WLKyBF0.

[154] Digital Rights Foundation. *Analysis: Personal Data Protection Bill 2023.*

protection draft, which has been heavily criticised and is still not finalised.[155] Even as a bill that is not specifically designed for social media data collection, this piece of legislation seems largely ineffective and riddled with loopholes for data protection in general.

Conclusion

In this chapter, the Facebook and YouTube privacy policies and by extension, the Meta and Google policies were critically analysed to understand certain core features of each social media platform's interaction with user data and its methods of collection or, in other words, surveillance. The analysis sought to establish which data is collected by each platform, how it is collected and processed, who can access it besides, where the data is stored and how much control users are allowed over their data. The analysis of each privacy policy demonstrated considerable overlap between both Facebook and YouTube's procedures for data collection and handling. However, it was apparent that YouTube, by association with Google, has greater access to data. Facebook, on the other hand, has a relatively more extensive policy with a focus on user-friendly explanations, accompanying illustrations, and videos.

The policy analyses, taken together with the previous chapter's study of secondary literature on the surveillance capitalism backed industry and social media user surveillance, allowed us a good understanding of what data collection and surveillance practices are used by Facebook and YouTube. Thenceforth, the chapter studied laws and policies in Pakistan that covered citizen's right to privacy in general, and specifically the question of their data privacy and confidentiality. It became apparent that while Pakistan has policies that touch upon data privacy and sovereignty, there is no dedicated policy for internet or social media surveillance which poses a direct threat to Pakistan's data from foreign actors. Similarly, the only piece of legislation under

[155] Media Matters for Democracy. "Data Protection and Online Safety Laws' Impact on Media & Digital Freedoms in Pakistan."

consideration, the draft of the Data Protection Bill 2023, while enforcing certain much needed laws against data controllers and processors, is still lacking in terms of specific provisions for challenges that arise from social media surveillance. It is clear that there is a need for further study and deliberation on the threats posed by methods of internet and social media user surveillance that must be sufficiently addressed in separate and specialised policies.

Chapter 4

CONCLUSIONS

This section will conclusively assess and discuss what this study has found in terms of research on social media user surveillance and its link to national security, with a special focus on Pakistani cyber security policy, as entailed by its research objectives. It will do so to address the study's main thesis question, which sought to understand whether existing cyber security policy in Pakistan is effective against threats posed by social media user surveillance. This chapter will first present a summary of the entire study, followed by the main research findings, verification of hypothesis and a final discussion.

4.5 Summary

To begin with, the literature review helped explore existing research on the themes of emerging challenges of surveillance capital and the big data industry, cyber threats proliferated by and present on social media, the current landscape of cyber security in Pakistan, and how social media can be used as a tool for intelligence. The review indicated that there is a gap in literature which can be bridged through more extensive research on data protection and citizen's privacy, specifically in connection with national security, and in the context of social media user surveillance. Moreover, literature on the subject which focuses on Pakistani cyber security and data protection is even rarer. By taking realism as its theoretical framework and applying the concept of data sovereignty—which many nation states, such as the US, Russia, China, Europe and others prioritise as part of their national cyber security policy—this study established the need for data protection against social media surveillance in Pakistan. Therefore, it became apparent that Pakistan too needs extensive and comprehensive research in the area of cyber surveillance in order to devise effective policy.

The second chapter of this study explored the concept of surveillance capitalism as an economic model that is behind the boom in data collection and manipulation as a business strategy, which without effective regulatory mechanisms, exposes data to vulnerabilities from countless fronts. From online retailers and banks to safety systems like car trackers and home locking mechanisms—every digital service collecting user data could potentially misuse the data or expose it to vulnerabilities by not storing it securely enough. Moreover, social media companies in particular also use data for business purposes such as profiling users, attention-grabbing, influencing opinions and manipulating behaviours, which pose their own set of ethical and safety issues. This means that in the era of surveillance capitalism, social media companies as well as most other businesses are incentivised to collect and further use data for profit, thus compromising user's privacy, right to choice, and overall national security.

The third chapter critically analysed the privacy policies of Facebook and YouTube, and by extension, parts of the general Meta and Google policies. The policy and terms of each platform was studied to specifically understand what data each platform collects and how, how the data is processed, who has access to it, where is it stored and finally, what are each company's user privacy control measures. The policies each had considerable overlap, with differences in scope of surveillance depending on the nature of each company's larger product and service ecosystem, as well as differences in presentation and accessibility of the policies. Lastly, the chapter highlighted certain laws that relate to the right of privacy of Pakistani citizens, and specifically considered the existing national cyber security policy as well as the only data protection legislation, the draft of the Data Protection Bill 2023 to assess where Pakistan stands in terms of effective regulation against social media user surveillance.

4.6 Research Findings

The findings of this research, which fall in line with its three research questions are as follows:

(i) What are the cyber security threats that emerge from social media user surveillance?

- Citizens'—including sensitive persons—data becomes vulnerable
- Citizens lack control over their own information
- Foreign companies and organisations then have greater access and knowledge of the citizens' information
- Data sovereignty is compromised
- The information and data can be used to gain crucial insight into trends within a nation's society
- This insight can then be used to conduct more effective and targeted information campaigns and behaviour modification agendas
- The value and use of data in the surveillance era makes it a national asset that needs protection

(ii) How effective is Pakistan's existing regulatory policy against cyber security threats posed by social media?

- The Constitution of Pakistan and its law recognise every citizen's right to privacy and right to access their data
- The National Cyber Security Policy 2021 implicitly outlines the importance of data sovereignty
- However, even together with the National Security Policy 2022, the cyber security policies in Pakistan do not address social media surveillance threats specifically
- The draft of the Data Protection Bill 2023 is the first of its kind to lay down regulations for data controllers and processors
- While, social media companies come under the categorisation of data controllers and processors, the bill is not enough to address the specific challenges and threats which emerge from social media user surveillance
- Moreover, as per critique offered by data rights experts, the bill, as it stands, has considerable loopholes and needs revision to be effective against any entity handling user data

(iii) Why does Pakistan need effective policy to address threats which emerge from social media user surveillance?

- To ensure that its citizens' as well as institutional data, including privileged data is secure and hence, not a liability to its national security
- To ensure its citizens' right to privacy and right to information
- To prevent and counter misinformation campaigns and behavioural change agendas from malicious actors
- Also, to make sure that alongside safe and protected use of social media, its citizens are able to utilize its economic benefits and thereby contribute to Pakistan's growth
- Finally, a comprehensive data policy is necessary for the state of Pakistan; its institutions and private sector included, to utilise data for its own advancement in accordance with conscious and best legal practices

4.7 Verification of Hypothesis

The hypothesis of this study posited that Pakistan can counter cyber security threats posed by social media user surveillance through effective cyber security policy. Where, the cyber security threats that emerge from social media user surveillance serve as the independent variable and the cause while the development of effective policy, in response to these threats, is the dependent variable and effect.

The findings of this study establish, in the first part, the various kinds of threats that emerge from social media companies' user surveillance practices. In the second part, it proves that existing cyber security policies are insufficient and cannot counter the threats. Therefore, the study verifies the hypothesis that there is a need to establish effective cyber security policy to address the threats resulting from social media companies' surveillance of Pakistani users.

4.8 Analysis

The findings of this study demonstrate, first and foremost, the need for effective policy, which is fundamentally essential to enact laws and enforce regulations that will protect citizen data and privacy.

This study has explored how protecting citizen data, which includes data of sensitive persons and organisations, are integral to Pakistan's national security, when the data of a country and its constituencies are considered a collective national asset. This is especially the case in the age of surveillance capitalism when all kinds of data and virtually all information is sought after by large corporations, political organisations, foreign agencies and many others to make use of for their own profit and in their own interest. When speaking of social media companies, we see that they are among the largest corporations with the greatest access to data that they not only make available to third parties such as foreign agencies, but also use it in ways that have a direct impact on users. This includes analysing user data to glean crucial and sensitive information about them such as their identification data, their pinpoint location and active movements, health data, financial data and more. Moreover, the large amounts of data also enable social media companies to not only influence users with marketing tactics, but to carry out or be used for targeted campaigns which are aimed at manipulating user behaviour. This can be seen in something as simple as a nation's youth becoming regressive and negatively influenced as a result of the deliberately designed addictive nature and overuse of social media, or it can even be politically motivated as is the case with many companies' selective censorship of content coming out of the ongoing Israeli attack on Palestine.

Among Pakistan's existing policy, the National Cyber Security Policy conceptualises data sovereignty and understands the need to protect data. However, given the scale at which social media companies operate and the particular threats they pose, it is imperative that a regulatory policy addresses social media companies separately.

Additionally, social media policy should go beyond the existing policies which only prioritise censorship and regulating content uploaded by local users. The critique of the data protection legislation in the pipeline, the Data Protection Bill 2023, also notes that the bill appears to prioritise state control while lacking accountability measures for government institutions, as well as a lack of understanding of how these foreign data processors function. Therefore, it is apparent that existing data protection policy and legal frameworks are not, as of yet, truly committed to regulating social media companies' data surveillance and use of local data. This becomes more evident, when Pakistan's policy is studied in comparison to other nations', such as China and the EU. In fact, a comparative critical analysis of data policies of different nations would be an insightful way to expand on this research and move further towards realising more effective policy for Pakistan.

Final Words

This chapter tied up the research by summarising all its sections and reporting its key findings. In doing so, it addressed the three main research questions of this study by establishing the primary cyber security threats which emerge from social media user surveillance and critically analysing the privacy policies of the two biggest social media platforms, Facebook and YouTube, and the existing policy as well as laws of Pakistan. In addition, when answering the first question, this research was able to establish a number of crucial concepts, such as the increased necessity for a data policy in the age of surveillance capitalism, the importance of data sovereignty, user data as a national asset, and the integral link between protection of a nation's data and national security. These findings then lend to the argument that an effective policy to regulate social media companies' surveillance practices is imperative to the national sovereignty and security of Pakistan. This is particularly the case when it is considered that the second part of the research found Pakistan's existing policy to be ineffective and in need of much reform. The way forward requires a need for more research on understanding the nature of social media, its surveillance and data practices, and a study of other nations' policies.

BIBLIOGRAPHY

Primary Sources

Facebook. "Privacy Checkup." Facebook, accessed 2 June 2024. https://www.facebook.com/privacy/checkup/.

Google. "Cloud Locations." Google Cloud accessed 2 June, 2024. https://cloud.google.com/about/locations.

Google. "Discover Our Data Center Locations." Google Data Center, accessed 2 June, 2024. https://www.google.com/about/datacenters/locations/?hl=en_US.

Google. "Global requests for user information." Google Transparency Report, accessed 1 June, 2024. https://transparencyreport.google.com/user-data/overview?hl=en_US.

Google. "Privacy Policy." Google Privacy and Terms, accessed 1 June. 2024.https://policies.google.com/privacy?hl=en-US

Google. "Terms of Service". YouTube Kids, accessed 1 June, 2024. https://kids.youtube.com/t/privacynotice.

Google. "Understanding the basics of privacy on YouTube apps." YouTube Help, accessed 1 June, 2024. https://support.google.com/youtube/answer/10364219?hl=en#zippy=%2C

Google. "Browse or delete your YouTube activity, and discover how your data makes YouTube and other Google services work better for you." Your data in YouTube, accessed 3 June, 2024. https://myaccount.google.com/u/0/yourdata/youtube?hl=en&pli=1.

Government of Pakistan. *The Prevention of Electronic Crimes Act 2016.* Islamabad: GoP, 2016. https://www.pakistancode.gov.pk/pdffiles/administrator6a061efe0ed5bd153fa8b79b8eb4cba7.pdf

Meta. "About Meta Advertising Standards." Business Help Centre. https://www.facebook.com/business/help/488043719226449?id=434838534925385.

Meta. "Ad preferences." Meta Accounts Centre, accessed 1 June, 2024. https://accountscenter.facebook.com/ads/.

Meta. "Government Requests for User Data." Transparency Center, accessed 1 June, 2024. https://transparency.meta.com/reports/government-data-requests.

Meta. “Meta Data Centers.” Data Centers at Meta, February 23, 2024. https://datacenters.atmeta.com/.

Meta. “Privacy Policy.” Meta Privacy Centre, 27 December, 2023. https://www.facebook.com/privacy/policy/?section_id=0-WhatIsThePrivacy.

Meta. “Privacy topics.” Meta Accounts Centre, accessed 2 June 2024. https://accountscenter.facebook.com/ads/

Meta, “Safety Resources for Parents.” Facebook Help Centre, accessed June 1, 2024, https://www.facebook.com/help/1079477105456277.

Ministry of Information Technology and Telecommunication. *CERT Rules 2023.* Islamabad: MoITT, 2023. https://pkcert.gov.pk/wp-content/uploads/2023/10/GAZETTE-CERT-Rules-2023.pdf.

Ministry of Information Technology and Telecommunication. *National Cyber Security Policy 2021.* Islamabad: MoITT, 2021. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf.

Ministry of Information Technology and Telecommunication. *Personal Data Protection Bill, 2023.* Islamabad: MoITT, 2023. https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf

National Security Division. *National Security Policy 2022.* Islamabad: National Security Division, 2022. https://dnd.com.pk/wp-content/uploads/2022/01/National-Security-Policy-2022-2026.pdf.

Secondary Sources

Abdulhamid, Shafii M., Sulaiman Ahmad, Victor O. Waziri, and Fatima N. Jibril. "Privacy and national security issues in social networks: the challenges." *International Journal of the Computer, the Internet and Management* 19, no. 3 (February 2014): 14-20. https://arxiv.org/ftp/arxiv/papers/1402/1402.3301.pdfAho, Brett, and Roberta Duffield. "Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China." Economy and Society 49, no. 2 (May 2020): 1-26. https://sci-hub.se/https://doi.org/10.1080/03085147.2019.1690275.

Anwar, Oves, Ayesha Malik, Abraze Aqil, and Noor F. Iftikhar. "Cyber Surveillance and Big Data-Pakistan's Legal Framework and the Need for Safeguards." *Research Society of International Law (RSIL) Law Review* 1, no. 35 (June 2020): 35-61. https://rsilpak.org/wp-content/uploads/2020/06/The-COVID-19-Law-Policy-Challenge-Cyber-Surveillance-and-Big-Data.pdf.

Awan, Mazhar Javed, Muhammad Haseeb Bilal, Awais Yasin, Haitham Nobanee, Nabeel Sabir Khan, and Azlan Mohd Zain. "Detection of COVID-19 in chest X-ray images: A big data enabled deep learning approach." *International journal of environmental research and public health* 18, no. 19 (September 2021). https://www.mdpi.com/1660-4601/18/19/10147

Ayoub, Amber, Kainaat Mahboob, A. Rehman Javed, Muhammad Rizwan, Thippa Reddy Gadekallu, Mustufa Haider Abidi, and Mohammed Alkahtani. "Classification and categorization of COVID-19 outbreak in Pakistan." Comput Mater Continua 69 (January 2021): 1253-69. https://www.researchgate.net/profile/Mustufa-Abidi/publication/352130166_Classification_and_Categorization_of_COVID-19_Outbreak_in_Pakistan/links/60bc6768299bf10dff9c89fb/Classification-and-Categorization-of-COVID-19-Outbreak-in-Pakistan.pdf

Brown, Ian. "Social media surveillance." 2015. https://onlinelibrary.wiley.com/doi/full/10.1002/9781118767771.wbiedcs122

Craig, Anthony, and Brandon Valeriano. "Realism and cyber conflict: Security in the digital age." In *Realism in Practice: An Appraisal*, edited by Davide Orsi, J. R. Avgustin and Max Nurnus, 85-101. Bristol: E-International Relations, 2018. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

Common Sense Privacy Program. Standard Privacy Report for Facebook. Common Sense Media, 2022. https://privacy.commonsense.org/privacy-report/Facebook.

Common Sense Privacy Program. Standard Privacy Report for YouTube. Common Sense Media, 2022. https://privacy.commonsense.org/privacy-report/YouTube.

Davies, Philip HJ. "Intelligence, information technology, and information warfare." *Annual Review of Information Science and Technology* 36 (2002): 313-52. https://sci-hub.se/https://doi.org/10.1002/aris.1440360108.

Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. "We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy." Paper presented at *Network and Distributed System Security (NDSS) Symposium 2019, San Diego, CA, USA, February, 24-27, 2019* (2018): https://doi.org/10.14722/ndss.2019.23378.

Digital Rights Foundation. Analysis: Personal Data Protection Bill 2023. Islamabad: DRF, 2023. https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf.

Edensor, Tim. *National identity, popular culture and everyday life*. London: Routledge.

2002.

Englehardt, Steven, Dillon Reisman, Christian Eubank, Peter Zimmerman, Jonathan Mayer, Arvind Narayanan, and Edward W. Felten. "Cookies that give you away: The surveillance implications of web tracking." *In Proceedings of the 24th International Conference on World Wide Web, pp. 289-299.* (2015). https://dl.acm.org/doi/pdf/10.1145/2736277.2741679.

Fuchs, Christian, and Daniel Trottier. "Towards a theoretical model of social media surveillance in contemporary society." *Communications* 40, no. 1 (March 2015): 113-135. https://westminsterresearch.westminster.ac.uk/download/c8923c6f244eb5a1fe92376cdee5cf6b967af4df315fc17109bc872bc94aeaf0/3293718/surv.pdf

Gay, Lorrie R., and P. Airasian. *Educational research: Competencies for analysis and applications*. New Jersey: Pearson, 2016.

Geelen, Max Edgar Floris. "Cyber Securitization and Security Policy." Master's diss.,

Leiden University, 2016. https://studenttheses.universiteitleiden.nl/access/item%3A2663862/view

Grundy, Quinn, Lindsay Jibb, Elsie Amoako, and Geoffrey Fang. "Health apps are designed to track and share." *bmj* 373 (June 2021): https://www.bmj.com/content/373/bmj.n1429.

Hammersley, Martyn. "Ethnography: problems and prospects." *Ethnography and education* 1, no. 1 (March 2016): 3-14. https://www.tandfonline.com/doi/full/10.1080/17457820500512697.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4: 1155-1175.

Hussain, Shabir, Farrukh Shahzad, and Adam Saud. "Analyzing the state of digital information warfare between India and Pakistan on Twittersphere." *SAGE Open* 11, no. 3 (July 2021): https://journals.sagepub.com/doi/pdf/10.1177/21582440211031905

Ibdah, Duha, Nada Lachtar, Satya Meenakshi Raparthi, and Anys Bacha. "“Why Should I Read the Privacy Policy, I Just Need the Service”: A Study on Attitudes and Perceptions Toward Privacy Policies." IEEE access 9 (November 2021): 166465-166487. https://ieeexplore.ieee.org/abstract/document/9624976.

Institute of Regional Studies (IRS), *Fake News: Unravelling the Greater Complexity of How Individuals, Institutions and the Whole Nations Manipulate Facts to Create Fake News to Their Advantage – Book of Peer-Reviewed Papers of International*

Conference on Fake News and Facts in Our Region Organised by the Institute of Regional Studies in Islamabad on April 24-26, 2019, (Islamabad: IRS, 2019).

Jacobsen, Knut A., and Kristina Myrvold. Religion and Technology in India. New York: Routledge, 2018.

Kemp, Simon. *Digital 2023: Global Overview Report.* Singapore: DataReportal, 2023. https://datareportal.com/reports/digital-2023-global-overview-report

Khalid, Zaki. "Examining the national security policy of Pakistan 2022-2026". *Centre for Strategic and Contemporary Research.* 2022. https://cscr.pk/explore/themes/defense-security/examining-the-national-security-poliensure the cy cy-of-pakistan-2022-2026/

Kröger, Jacob Leon, and Philip Raschke. "Is my phone listening in? On the feasibility and detectability of mobile eavesdropping." In Data and Applications Security and Privacy XXXIII: 33rd Annual IFIP WG 11.3 Conference, DBSec 2019, Charleston, SC, USA, July 15–17, 2019, Proceedings 33, pp. 102-120. *Springer International Publishing,* 2019.

Kuehn, Andreas. "Cookies versus clams: Clashing tracking technologies and online privacy." info 15, no. 6 (September 2013): 19-31. https://sci-hub.et-fine.com/10.1108/info-04-2013-0013.

Lim, Kevjn. "Big data and strategic intelligence." *Intelligence and National Security* 31, no. 4 (June 2016): 619-635. https://sci-hub.se/https://doi.org/10.1080/02684527.2015.1062321.

Liu, Lizhi. "The rise of data politics: digital China and the world." *Studies in Comparative International Development* 56 (March 2021): 45-67. https://link.springer.com/article/10.1007/s12116-021-09319-8.

Lyon, David. "Surveillance, Snowden, and big data: Capacities, consequences, critique." *Big data & society* 1, no. 2 (July 2014): 1-13. https://doi.org/10.1177/2053951714541861.

Malik, Aqab. "Strategic Communication – A Synchronised Effort for Information Dissemination by Pakistan." *SAGE International,* (2011): https://pdfs.semanticscholar.org/0665/477fa5d7b7fdb50e57cb53112e900ba2b7b7.pdf

Maltby, Dylan. "Big data analytics." Paper presented at *74th Annual Meeting of the Association for Information Science and Technology (ASIST),* New Orleans, N.O., USA, October 7 – 12, 2011. https://shorturl.at/otcOX.

Marti, Don, Fengyang Lin, Matthew Schwartz and Ginny Fahs. *Who Shares Your*

Information With Facebook? Sampling the Surveillance Economy in 2023. New York: Consumer Reports, 2023. https://innovation.consumerreports.org/wp-content/uploads/2024/01/CR_Who-Shares-Your-Information-With-Facebook.pdf.

Media Matters for Democracy. “Data Protection and Online Safety Laws' Impact on Media & Digital Freedoms in Pakistan.” July 31, 2023, legal analysis, 58:40, https://www.youtube.com/watch?v=0wn7WLKyBF0.

Meta. “Meta Reports Fourth Quarter and Full Year 2023 Results; Initiates Quarterly Dividend.” Meta Press Release, February 1, 2024. On the Meta website. https://investor.fb.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx.

Minocher, Xerxes, and Caelyn Randall. "Predictable policing: New technology, old bias, and future resistance in big data surveillance." *Convergence* 26, no. 5-6 (2020): 1-17. https://journals.sagepub.com/doi/abs/10.1177/1354856520933838

Mitchell, Damion, and Omar F. El-Gayar. "The effect of privacy policies on information sharing behavior on social networks: A Systematic Literature Review." Paper presented at *the 53rd Hawaii International Conference on System Sciences, Maui, Hawaii, USA, January, 7-10, 2020.* https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1230&context=bispapers

Noor, Saba, Waseem Akram, and Touseef Ahmed. "Predicting COVID-19 incidence using data mining techniques: a case study of Pakistan." *Broad Research in Artificial Intelligence and Neuroscience* 11, no. 4 (February 2020): 168-184. https://www.researchgate.net/publication/347858382_Predicting_COVID-19_Incidence_Using_Data_Mining_Techniques_A_case_study_of_Pakistan

Omand, David, Jamie Bartlett, and Carl Miller. "Introducing social media intelligence (SOCMINT)." *Intelligence and National Security* 27, no. 6 (July 2012): 801-823. https://sci-hub.se/https://doi.org/10.1080/02684527.2012.716965

OOSGA. *Social Media in Pakistan – 2023 Stats and Platform Trends.* Singapore: OOSGA, 2023. https://oosga.com/social-media/pak/

Pakistan Telecommunication Authority. *Annual Report 2023.* Islamabad: PTA, 2024. https://www.pta.gov.pk/assets/media/pta_annual_report_12022024.pdf

Pickin, Matthew. "What is the securitization of cyberspace? Is it a problem." 2014. Academia. https://www.academia.edu/3100313/What_is_the_securitization_of_cyberspace_Is_it_a_problem

Pohle, Julia, and Thorsten Thiel. "Digital sovereignty." *Internet Policy Review* 9, no.4 (December 2020). https://policyreview.info/concepts/digital-sovereignty

Qin, Bei, David Strömberg, and Yanhui Wu. "Why does China allow freer social media? Protests versus surveillance and propaganda." *Journal of Economic Perspectives* 31, no. 1 (2017): 117-140. https://pubs.aeaweb.org/doi/pdf/10.1257/jep.31.1.117

Roski, Joachim, George W. Bo-Linn, and Timothy A. Andrews. "Creating value in health care through big data: opportunities and policy implications." *Health affairs* 33, no. 7 (2014): 1115-1122. https://sci-hub.et-fine.com/10.1377/hlthaff.2014.0147

Saud, Adam, and Nehal Kazim. "Disinformation and Propaganda Tactics: Impact of Indian Information Warfare on Pakistan." *Journal of Indian Studies* 8, no. 2 (December 2022): 335-354. http://pu.edu.pk/images/journal/indianStudies/PDF/9_v8_2_22.pdf

Shaikh, Muneeb Imran. "Pakistan's Cybersecurity Policy in 2021: A Review." ISACA, 24 November, 2024. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-39/pakistan-cybersecurity-policy-in-2021-a-review.

Stritzel, Holger. "Securitization and The Copenhagen School." In *Security in translation: Securitization theory and the localization of threat,* edited by Stuart Croft, 11-36. London: Palgrave Macmillan, 2014.

Su, Chunmeizi, and Wenjia Tang. "Data sovereignty and platform neutrality–A comparative study on TikTok's data policy." *Global Media and China* 8, no. 1 (February 2023): 57-71. https://journals.sagepub.com/doi/full/10.1177/20594364231154340.

Syed, Rubab, Ahmed A. Khaver, and Muhammad Yasin. "Cyber security: Where does Pakistan stand?" *Sustainable Development and Policy Institute (SDPI) Publications,* working paper no. 167, Islamabad: SDPI, February 14, 2019: 1-15. https://sdpi.org/cyber-security-where-does-pakistan-stand-w-167/publication_detail.

Trottier, Daniel. "A research agenda for social media surveillance." *Fast Capitalism* 8, no. 1 (2011): 59 - 68.

Ullah, Atta, Chen Pinglu, Saif Ullah, Hafiz Syed Mohsin Abbas, and Saba Khan. "The role of e-governance in combating COVID-19 and promoting sustainable development: a comparative study of China and Pakistan." *Chinese Political Science Review* 6, no. 1 (November 2021): 86-118. https://link.springer.com/article/10.1007/s41111-020-00167-w.

Vatanparast, Roxana. "Data governance and the elasticity of sovereignty." *Brook. J. Int'l L.* 46 (May 2021): 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839847

White, Candace L., and Brandon Boatwright. "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations." *Public Relations Review* 46, no. 5 (December 2020): https://www.sciencedirect.com/science/article/abs/pii/S0363811120301077.

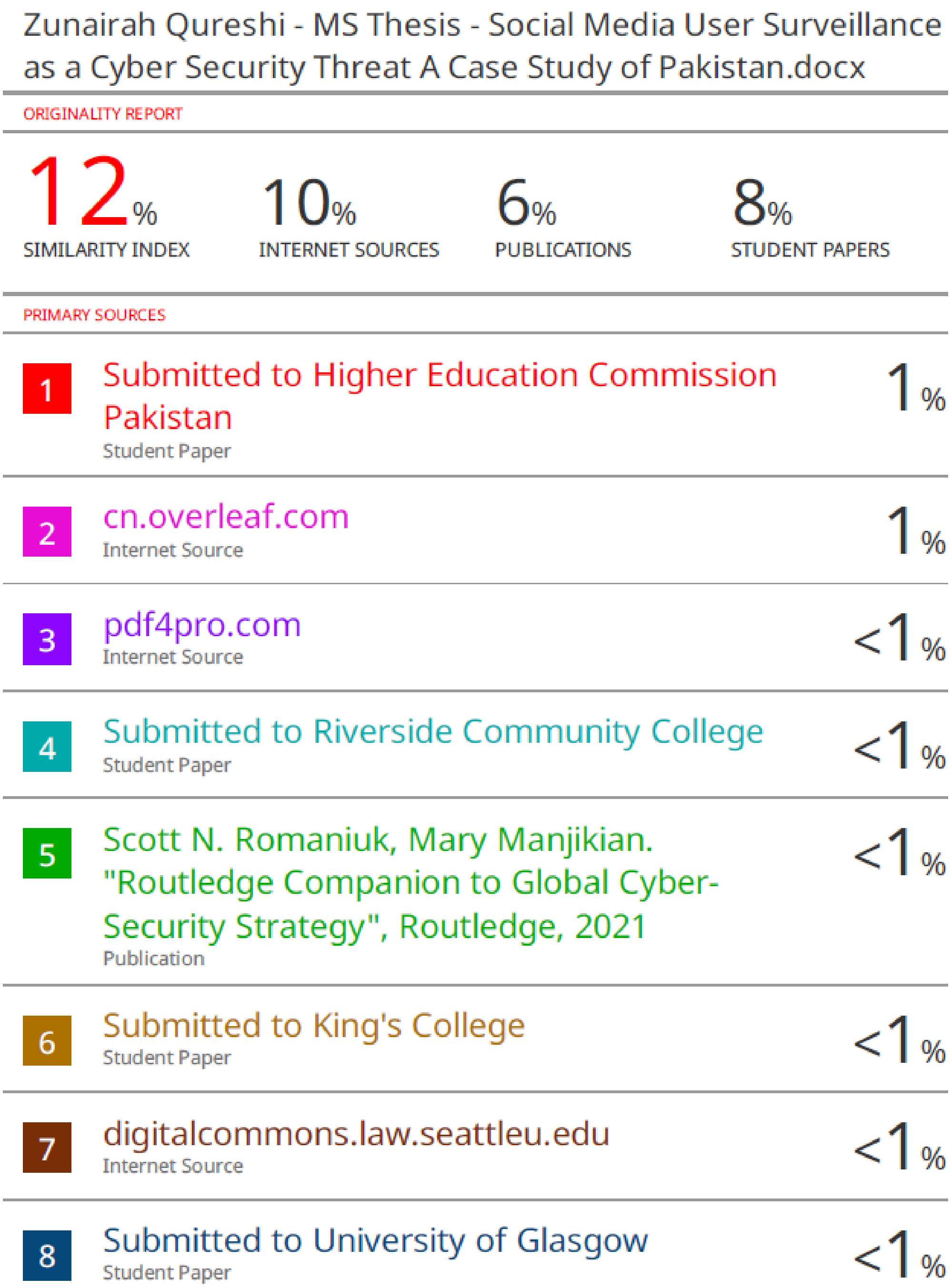
Wong, Carey. "Smartphone location-based services in the social, mobile, and surveillance practices of everyday life." *Media@LSE MSc Dissertation Series* (2014): https://www.lse.ac.uk/media-and-communications/assets/documents/research/msc-dissertations/2013/96-Wong.pdf

Wuhan University, China Center for Information Industry Development, Beijing Institute of Technology, Southwest University of Political Science & Law, University of International Business and Economics, Tsinghua University, National Institute for Global Strategy, Chinese Academy of Social Sciences, et al. "Sovereignty in Cyberspace: Theory and Practice (Version 4.0)." *World Internet Conference,* January 16, 2024. https://subsites.chinadaily.com.cn/wic/2024-01/16/c_956165.htm.

Xu, Lei, Chunxiao Jiang, Jian Wang, Jian Yuan, and Yong Ren. "Information security in big data: privacy and data mining." *Ieee Access* 2 (October 2014): 1149-1176. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6919256

Yamin, Tughral. "Cyberspace Management in Pakistan." *Governance and Management Review* 3, no. 1 (January 2018): 46-61. https://pu.edu.pk/images/journal/IAS/PDF/4-v3_1_18.pdf.

Zuboff, Shoshana. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books. 2019.



Zunairah Qureshi - MS Thesis - Social Media User Surveillance as a Cyber Security Threat A Case Study of Pakistan.docx

ORIGINALITY REPORT

12%	10%	6%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Higher Education Commission Pakistan Student Paper	1%
2	cn.overleaf.com Internet Source	1%
3	pdf4pro.com Internet Source	<1%
4	Submitted to Riverside Community College Student Paper	<1%
5	Scott N. Romaniuk, Mary Manjikian. "Routledge Companion to Global Cyber-Security Strategy", Routledge, 2021 Publication	<1%
6	Submitted to King's College Student Paper	<1%
7	digitalcommons.law.seattleu.edu Internet Source	<1%
8	Submitted to University of Glasgow Student Paper	<1%