



Kurt, Seher (2026) *Digital governance of social media platforms: a comparative study of India and the United Kingdom*. PhD thesis.

<https://theses.gla.ac.uk/85838/>

Copyright and moral rights for this work are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This work cannot be reproduced or quoted extensively from without first obtaining permission from the author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

Enlighten: Theses

<https://theses.gla.ac.uk/>
research-enlighten@glasgow.ac.uk



University
of Glasgow

**Digital Governance of Social Media Platforms:
A Comparative Study of India and the United Kingdom**

Seher Kurt

Submitted in fulfilment of the requirement of the Degree of
Doctor of Philosophy

School of Social and Political Sciences
College of Social Sciences
University of Glasgow

February 2025

Abstract

This thesis makes a timely contribution to the interdisciplinary field of digital governance by examining its construction in relation to social media platforms (SMPs) in India and the United Kingdom (UK).

The adaptation of nation-state governance into digital governance accelerated from the mid-1990s with the rise of the internet and expanded in the 2000s with Web 2.0 and SMPs. They prompted creation of new laws and regulations, developed new technologies, and transformed public participation in the digital sphere. Unlike traditional state-centric governance, digital governance operates within a multi-stakeholder environment that is shaped by the intertwined engagement of various actors, including states, companies, users, and technology. To explain this, the thesis introduces ‘the structuration model of digital governance’, highlighting the interplay of technology, structure, and agency in different contexts. This framework offers a holistic approach to study the complexities of digital governance in the two countries.

Acknowledging nondemocratic actions of democratic states in the digital governance literature, this research project sought to understand: ‘How do India and the UK construct their digital governance in relation to social media platforms?’ And ‘What is the broader significance of this for democracies and digital governance?’ To address these, three sets of sub-research questions were formulated: (1) What are the existing digital dual-use operations involving social media platforms in India and the UK? Who conducts these operations? (2) How do legal frameworks inform the regulation of digital dual-use operations and stakeholders? What legal concerns are raised regarding the digital governance of social media platforms? (3) What implications and concerns do experts raise regarding the digital governance of social media platforms and their impact on the public of India and the UK?

To answer these questions, this research employed a comparative case study design. It focused on two democracies’ digital governance, India and the UK, through two SMPs, Facebook and Twitter. It adopted a multimethod design consisting of three stages: (1) secondary analysis of Freedom on the Net and

transparency reports from Facebook and Twitter, (2) 22 semi-structured online interviews with digital rights activists, journalists, lawyers, and experts, and (3) theme synthesis and data source triangulation for validation. This analysis generated three themes — -veillance, content control, and shaped discourse — each of which examined four aspects of digital governance: operations, the role of social media platforms, legal frameworks, and experts' concerns and views of their influence on the public. My findings revealed that both countries had both digitally democratic and authoritarian features in how they governed SMPs, leading to development of the digital hybrid regime concept. By distinguishing state governance from digital governance, I identified three categories of digital hybrid regime: democratic-digital hybrid, full-scale digital hybrid, and authoritarian-digital hybrid. Based on my empirical findings, I classified India as a full-scale hybrid and the United Kingdom as a democratic-digital hybrid regime.

This thesis advances understanding of the complex nature of digital governance, acknowledging the divergence between political regimes at state and digital levels. It bridges the gap between digital democracy and authoritarianism, reigniting discussions on democratic backsliding and contributes to hybrid regimes in the digital sphere.

Table of Contents

Abstract	2
Table of Contents	4
List of Tables	9
List of Figures	10
Acknowledgement.....	11
Author's Declaration.....	12
Abbreviations	13
General Abbreviations	13
Abbreviations Specific to India.....	13
Abbreviations Specific to the United Kingdom	13
Chapter 1 Introduction	15
1.1 Overview	15
1.2 Research Purpose	16
1.2.1 Why Study the Digital Governance of Social Media Platforms in Two Democracies?....	17
1.2.2 What are Social Media Platforms and Why are They the Focus of This Research?.....	18
1.2.3 What are Dual-use Technologies and Why do They Matter?	21
1.3 Research Aim and Objectives.....	24
1.4 Key Contributions of the Thesis	25
1.5 Thesis Structure	27
Chapter 2 Literature Review.....	28
2.1 Democracy.....	29
2.1.1 Digital Democracy	30
2.2 Authoritarianism	34
2.2.1 Digital Authoritarianism	36
2.3 Discussion: Forms of Digital Governance	43
2.4 Conclusion	44
Chapter 3 Contextual Insights from India and the United Kingdom.....	46
3.1 State and Digital Demographics of India and the UK	46
3.2 Political System	47
3.2.1 Form of Government	48
3.2.2 Party Politics	49
3.2.3 Elections.....	50
3.3 Social Diversity.....	52
3.3.1 Gender (In)equality in Political Participation	52
3.3.2 Understanding Minority Groups	53
3.3.3 The Effectiveness of Civil Society Organisations	54

3.4	A Brief Historical Context: 2019-2023.....	56
3.4.1	Key Changes and Incidents	56
3.4.2	Freedom in the World versus Freedom on the Net.....	58
3.5	Conclusion	59
Chapter 4	<i>Analytical Framework</i>.....	60
4.1	Liberal Internationalism	60
4.2	Structuration Model of Digital Governance	62
4.2.1	Structuration Theory: Anthony Giddens	62
4.2.2	The Duality of Technology: Jane Orlikowski	65
4.2.3	Interpretative Research: Geoff Walsham	66
4.2.4	Creating ‘the Structuration Model of Digital Governance’ in India and the UK	67
4.3	Conclusion	72
Chapter 5	<i>Research Design and Methodology</i>.....	73
5.1	Philosophical Underpinnings of my Interdisciplinary Research	73
5.2	Research Questions	75
5.3	Research Design: Comparative Case Study	76
5.4	Qualitatively Driven Multimethod Approach	78
5.5	Methods.....	81
5.5.1	Stage 1: Secondary Data Analysis.....	81
5.5.2	Stage 2: Semi-structured Online Interviews	87
5.5.3	Stage 3: Synthesis and Validation.....	98
5.6	Ethical Considerations	100
5.7	Limitations	102
5.8	Conclusion	104
Chapter 6	<i>-Veillance in India and the UK</i>.....	105
6.1	The Socio-Political Landscape of -Veillance Operations.....	106
6.1.1	India	106
6.1.2	United Kingdom	112
6.2	The Role of Social Media Platforms on -Veillance	117
6.2.1	India	117
6.2.2	United Kingdom	123
6.3	The Legal Frameworks on -Veillance.....	130
6.3.1	India	130
6.3.2	United Kingdom	137
6.4	Experts’ Concerns and Views on the Implications of -Veillance on the Public 143	
6.4.1	India	143
6.4.2	United Kingdom	151
6.5	Conclusion	158

Chapter 7	<i>Content Control in India and the UK</i>	162
7.1	The Socio-Political Landscape of Content Control Operations	164
7.1.1	India	164
7.1.2	United Kingdom	166
7.2	The Role of Social Media Platforms on Content Control	169
7.2.1	India	169
7.2.2	United Kingdom	176
7.3	The Legal Frameworks on Content Control	181
7.3.1	India	181
7.3.2	United Kingdom	188
7.4	Experts' Concerns and Views on the Implications of Content Control on the Public	195
7.4.1	India	195
7.4.2	United Kingdom	202
7.5	Conclusion	208
Chapter 8	<i>Shaped Discourse in India and the UK</i>	212
8.1	The Socio-Political Landscape of Shaped Discourse Operations	213
8.1.1	India	213
8.1.2	United Kingdom	216
8.2	The Role of Social Media Platforms in Shaped Discourse	219
8.2.1	India	219
8.2.2	United Kingdom	227
8.3	The Legal Frameworks on Shaped Discourse	235
8.3.1	India	235
8.3.2	United Kingdom	240
8.4	Experts' Concerns and Views on the Implications of Shaped Discourse on the Public	246
8.4.1	India	246
8.4.2	United Kingdom	256
8.5	Conclusion	265
Chapter 9	<i>Discussion</i>	269
9.1	Digital Dual-use Operations Involving Social Media Platforms in India and the UK	269
9.1.1	-Veillance	269
9.1.2	Content Control	275
9.1.3	Shaped Discourse	279
9.1.4	Summary	286
9.2	Legal Frameworks and Concerns about the Regulation of Digital Dual-Use Operations and Stakeholders in India and the UK	289
9.2.1	-Veillance	289

9.2.2	Content Control	293
9.2.3	Shaped Discourse	297
9.2.4	Summary	303
9.3	Experts' Views and Concerns about the Implications of Digital Governance for the Indian and UK Public	307
9.3.1	-Veillance	307
9.3.2	Content Control	310
9.3.3	Shaped Discourse	312
9.3.4	Summary	315
9.4	Digital Governance of Social Media Platforms in India and the UK: Structure and Political Regime	318
9.4.1	Digital Governance Structure: Empirical and Theoretical Perspectives.....	318
9.4.2	Digital Governance Regimes in India and the UK, and the Emergence of a Digital Hybrid Regime	324
9.5	Conclusion	326
Chapter 10	Conclusion.....	327
10.1	Digital Hybrid Regimes	327
10.1.1	'Digital Hybrid Regime' as a New Concept in Digital Governance	327
10.1.2	Three Types of Digital Hybrid Regimes (DHRs)	333
10.1.3	Digital Hybrid Regimes in India and the UK	338
10.2	Research Reflections	341
10.2.1	Contributions.....	341
10.2.2	Policy Recommendations for Digital Governance	343
10.2.3	Limitations	345
10.2.4	Recommendations for Further Studies	346
10.3	Concluding Remarks	346
Appendices		350
Appendix 1: Freedom in the World (2020-2022).....		350
Appendix 2: Freedom on the Net (2019-2021)		353
Appendix 3: FoN Reports' Codes and Themes		356
Theme 1: Internet Disruption		356
Theme 2: Content Control		357
Theme 3: -Veillance		358
Appendix 4: Legal Extracts and Notes		359
4.1	The Universal Declaration of Human Rights (1948)	359
4.2	Indian Legislation	359
4.3	UK legislation	367
Appendix 5: India-Facebook: Government Requests for User Data.....		373
Appendix 6: India-Twitter: Government Information Requests		374
Appendix 7: UK-Facebook: Government Requests for User Data.....		375

Appendix 8: UK-Twitter: Government Information Requests	376
Appendix 9: India-Facebook: Content Restrictions.....	377
Appendix 10: India-Twitter: Removal Requests	378
Appendix 11: UK-Facebook: Content Restrictions	379
Appendix 12: UK-Twitter: Removal Requests	380
Appendix 13: Participant Information Sheet.....	381
Appendix 14: Privacy Notice.....	383
Appendix 15: Consent Form	385
Appendix 16: Six Themes from the Second Stage	387
Appendix 17: Final Themes	392
<i>Bibliography</i>	<i>394</i>

List of Tables

Table 5.1: Participants from India	89
Table 5.2: Participants from the UK.....	90
Table 6.1: -Veillance.....	106
Table 6.2: % of data produced from Facebook-India.....	120
Table 6.3: Compliance rate of Twitter-India.....	121
Table 6.4: % of data produced by Facebook-UK	127
Table 6.5: Compliance rate of Twitter-UK	127
Table 7.1: Content Control	163
Table 7.2: Compliance rate of Twitter-India.....	172
Table 7.3: Compliance rate of Twitter-UK	179
Table 8.1: Shaped Discourse	213
Table 9.1: Summary of -veillance operations	270
Table 9.2: Summary of data/information requests from Facebook and Twitter (2019-2021)	273
Table 9.3: Summary of content control operations	275
Table 9.4: Summary of content removals from Facebook and Twitter (2019-2021)	277
Table 9.5: Summary of shaped discourse operations	279
Table 9.6: Summary of legal frameworks on -veillance	289
Table 9.7: Summary of legal frameworks on content control	293
Table 9.8: Summary of legal and government frameworks on shaped discourse	297
Table 9.9: Summary of views and concerns regarding -veillance	307
Table 9.10: Summary of views and concerns regarding content control.....	310
Table 9.11: Summary of views and concerns regarding shaped discourse	312

List of Figures

Figure 2.1: Scopus (2023b) search on ‘digital AND democracy’	31
Figure 2.2: Scopus (2023a) search on ‘digital AND authoritarianism’	36
Figure 4.1: Structuration model of digital governance of social media platforms	70
Figure 5.1: Multimethod comparative case study design.....	80
Figure 6.1: Government requests for user data: total requests.....	117
Figure 6.2: Government information requests: total requests (India-Twitter) .	118
Figure 6.3: Government total requests vs number of accounts requested (India- Facebook).....	119
Figure 6.4: Government total requests vs accounts specified (India-Twitter) ..	119
Figure 6.5: % data produced (user account) (India-Facebook)	120
Figure 6.6: Accounts specific compliance (India-Twitter)	121
Figure 6.7: Government requests for user data: total requests (UK-Facebook) .	124
Figure 6.8: Government information requests: total requests (UK-Twitter)	125
Figure 6.9: Government total requests vs number of accounts requested (UK- Facebook).....	125
Figure 6.10: Government total requests vs accounts specified (UK-Twitter) ...	126
Figure 6.11: % data produced (user account) (UK-Facebook).....	127
Figure 6.12: Account specific compliance (UK-Twitter).....	128
Figure 7.1: Amount of content restricted based on local law (India-Facebook)	Error! Bookmark not defined.
Figure 7.2: Restrictions by product (Facebook-India).....	171
Figure 7.3: Combined legal demands & accounts specified (India-Twitter).....	171
Figure 7.4: Amount of content restricted based on local law (UK-Facebook) ..	177
Figure 7.5: Restrictions by product (UK-Facebook)	177
Figure 7.6: Combined legal demands & accounts specified (UK-Twitter)	178
Figure 9.1: The three empirical aspects of digital governance	319
Figure 9.2: Structuration model of digital governance of social media platforms	320
Figure 10.1: Severity of digital hybrid regimes	338

Acknowledgement

Undertaking a PhD has been one of the greatest challenges of my life. Beginning this journey amid the uncertainties of the Covid-19 pandemic was stressful, yet it marked the start of a journey that continues to excite me (even after four years). As I celebrate this milestone with happiness, I am extremely grateful to those who have supported me throughout this journey.

First, I express my deepest gratitude to my main supervisor Prof. Bridgette Wessels and my secondary supervisors Prof. Martin Kretschmer and Prof. Andrew Hoskins. Pursuing an interdisciplinary project presented significant challenges and was only possible with your expertise, guidance, and support.

I extend my gratitude to my parents, Adil Aydin Kurt and Ozlem Kurt, my siblings, and friends who were always there for me, especially at difficult times. This journey was full of ups and downs, which I would not have been able to complete without your unwavering support.

Lastly, I would like to thank the University of Glasgow for this opportunity and support throughout my degree and my interview respondents from India and the United Kingdom, who I am indebted to for their interest in taking part in my research. The findings of this thesis would be missing without their involvement.

Author's Declaration

I declare that, except explicit reference is made to the contribution of others, that this dissertation is the result of my own work and has not been submitted for any other degree at the University of Glasgow or any other institution.

Printed Name: Seher Kurt

Signature: 

Abbreviations

General Abbreviations

EU	European Union
FiW	Freedom in the World
FoN	Freedom on the Net
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
ISP	Internet Service providers
MP	Member of Parliament
MSP	Mobile Service Providers
PM	Prime Minister
SMP	Social Media Platforms
SORM	System of Operative Investigative Measures
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
URL	Uniform Resource Locator
US	United States
VPN	Virtual Private Network
WW	World Wars
WWW	World Wide Web

Abbreviations Specific to India

AASMA	Advanced Application for Social Media Analytics
BJP	Bharatiya Janata Party
CAA	Citizenship Amendment Act
CMS	Central Monitoring System
INC	Indian National Congress
IPC	Indian Penal Code
IT Act	Information Technology Act
LIM	Lawful Intercept and Monitoring
MEITY	Ministry of Electronics and Information Technology
NATGRID	National Intelligence Grid
NETRA	Network Traffic Analysis
RTI	Right to Information

Abbreviations Specific to the United Kingdom

DCMS	Digital, Culture, Media and Sport
DPA	Data Protection Act
ECHR	European Convention on Human Rights
GCHQ	The Government Communications Headquarters
IP Act	Investigatory Power Act
IWF	Internet Watch Foundation
Met Police	Metropolitan Police
OFBJP-UK	Overseas Friends of the BJP (UK)

Ofcom	The Office of Communications
ONS	Office for National Statistics
OSB	Online Safety Bill
RIPA	Regulation of Investigatory Powers Act
RRU	Rapid Response Unit
SOCMINT	Social Media Intelligence

Chapter 1 Introduction

This chapter introduces my research on the ‘Digital Governance of Social Media Platforms: A Comparative Study of India and the United Kingdom’. As the title suggests, this study integrates concepts of digital governance and social media platforms in two democratic countries. While this combination highlights the originality and uniqueness of my research, it also presents a complex and multidimensional framework. To provide clarity, this chapter is divided into five sections: overview, research purpose, research aim and objectives, key contributions of the thesis and thesis structure.

1.1 Overview

Digital governance encompasses both digital technologies - which extend beyond the internet and include other technological foundations like information and communication technologies (ICTs), big data, and platforms - and governance, involving multiple actors in addition to states (Flyverbom *et al.*, 2019; Komaitis and Carter, 2023). While digital governance is broader than the internet, its proliferation since 1993¹ has played a central role in global expansion. By 2019, more than half the world’s population, 4.3 billion out of 7.8 billion, had access to the internet (Kemp, 2019; Worldometer, n.d.). Despite its stateless and decentralised nature described in the literature (Piccone, 2017), the internet’s expansion has driven states to territorialise the digital sphere by adapting their governance frameworks, regardless of their political regimes. Although their adaptation has varied in relation to different factors like technological advancements, economic capabilities, and political regimes, digital integration into the public sector has become inevitable (Torfinng *et al.*, 2020).

Throughout history, various governance models have emerged, including democracy, republic, monarchy, feudalism, communism, parliamentary and presidential systems. However, there is no standard accepted definition of governance in the literature. From a constructivist ontology, governance is an outcome of a socially constructed process that is shaped by the ruling

¹ The internet was invented in 1983 but made available to the public in 1993.

mechanism and socio-economic interactions of key actors and stakeholders in a society (Colebatch, 2014). Constructivists perceive technological transformation to be influenced by individual actions as well as social, political and legal frameworks that have arisen in states (Hague and Loader, 1999, p. 4). This explains diverse technological enactments and approaches to digital governance, which further lead to scholarly literature on optimistic and pessimistic views of its integration into governance.

The optimistic viewpoint sees technological transformations as advancing democracy and liberating citizens, especially in repressive regimes. Diamond (2010, p. 70) referred to the internet and emerging ICTs, including SMPs, as liberation technologies which ‘expand political, social, and economic freedom’ to counter authoritarian regimes and move their countries closer to democracy. Similarly, Piccone (2017, p. 2) pointed out that digital channels have given people ‘opportunities to exercise their rights to freedom of expression and association, to participate in civic life, and hold public officials accountable’. In contrast, the pessimistic viewpoint argues that digital integration strengthens state control. Scholars contend that governments, as dynamic organisations, quickly adapt and turn opportunities to their own benefit (MacKinnon, 2012; Gunitsky, 2015). This can be supported with recent studies which show increasing governmental control of the internet, including information control, surveillance monitoring and propaganda spreading (Kawerau *et al.*, 2023). This has resulted in the emergence of digital authoritarianism, whilst also creating problems of ‘access, privacy, and surveillance’, even in democratic states (Chadwick, 2006, p. 178).

Together, these divergent viewpoints illustrate how technological developments can be interpreted and utilised in different ways. This not only highlights the importance of the socio-political context in which digital governance is studied, but also underscores its dual-use potential, as explained in the next section.

1.2 Research Purpose

This section outlines the purpose of my research by addressing three key questions in the following subsections: 1) Why study the digital governance of social media platforms in two democracies?, 2) What are social media platforms

and why were they the focus of this research?, and 3) What are dual-use technologies and why do they matter?

1.2.1 Why Study the Digital Governance of Social Media Platforms in Two Democracies?

SMPs have become central to discussions of digital governance and contemporary politics. Events such as the Arab Spring (2010), the Snowden data leaks (2013), and the Cambridge Analytica scandals (2018) exposed a connection between SMPs and their real-world consequences, such as revolutionary movements, governments' secret operations, and election manipulation. Acknowledging that the latter two incidents occurred in democracies, the US and the UK, reveal how democracies undermined their own narratives, while illustrating digital authoritarian tendencies. Consequently, debates over the weakening of digital democracy and the increase in digital authoritarianism have intensified. Longitudinal studies by Freedom House reflect this, showing a ninth consecutive year of declining global internet freedom in 2019 (Shahbaz and Funk, 2019). Their annual report highlighted that SMPs were becoming illiberal for various reasons, including surveillance, misinformation and disinformation, and their limiting of freedom of expression (Shahbaz and Funk, 2019). These ongoing shifts have created a complex problem of digital governance, combining governance and technology.

The governance aspect of these challenges can be explained through arguments around democracies' increasing reliance on 'national security' to justify and legitimise their actions (MacAskill, 2014; Michaelsen, 2018b; Michaelsen, 2018a; Morgus, 2019; Wright, 2019; Liu, 2020; Yayboke and Brannen, 2020; Krekó, 2021; Brandt, 2022). I explain this through the theory of securitisation. Securitisation refers to the act of 'presenting an issue as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure' (Buzan *et al.*, 1997, p. 24). As a socially constructed process, it involves an actor performing a speech act about an existential threat directed at an audience (Buzan *et al.*, 1997). This framing enables extraordinary measures being made acceptable to the public, like the world-wide increasing of security measures for national security reasons after the 9/11 terror attacks in the US, including digital measures (like surveillance) (see Chapter 2 for more

detail). Thus, securitisation emphasises how political actors justify exceptional actions in response to perceived threats.

The technological side can be explained through big technology companies' proximity to political processes in democracies, especially during elections. Scholars such as Kreiss and McGregor (2017) demonstrate how firms like Facebook, Google, and Twitter provided strategic support to political campaigns, highlighting their role as active agents rather than neutral platforms during elections. This reflects platforms' active role in mediating and shaping political communication. Kreiss and McGregor (2017) further argue that this proximity is underpinned by mutual interest and trust, risking the politicisation of the SMP environment and influencing their regulation depending on the context. This not only creates a question of neutrality among platforms, but also raises issues over transparency, accountability, and democratic integrity in how SMPs get regulated by states.

Together, states justified use of technologies and the proximity of technology companies raise significant concerns about real-life implications of the digital sphere, especially in socio-political contexts. Acknowledging that such incidents occur in countries irrespective of political regime underscores that challenges in digital governance also emerge within democracies, despite their strong principles in rights, transparency, and accountability. Given these dynamics, the purpose of this research was to objectively compare two democracies to understand the contexts behind their digital governance operations. To achieve this, it focused particularly on SMPs, as the next subsection explains.

1.2.2 What are Social Media Platforms and Why are They the Focus of This Research?

I address these questions by presenting an overview of SMPs' historical creation, providing scholarly definition, and explaining their relevance to my research. To explain the emergence of SMPs, I outline the phases of the Web development. Whilst the internet was invented in 1983 and made available to the public in 1993, the World Wide Web (WWW) has evolved from Web 1.0 to Web 2.0 and, as some scholars argue, to Web 3.0. Starting from the early 1990s, Web 1.0 had

limited user engagement and focused on delivering the requested page to a reader (O'Reilly, 2007). Web 2.0, which began in the early 2000s, introduced interactive features such as user-generated content, engaging in online dialogue, and gathering information from online sources (O'Reilly, 2007; Allen, 2013; Rudman and Bruwer, 2016; Lindgren, 2022). However, SMPs are dynamic and rapidly evolve within Web 2.0 itself. While Myspace and Friendster were among the most popular platforms in the early 2000s, platforms like Facebook, YouTube, WhatsApp, WeChat, Instagram, and Twitter were trending when I began my research in 2019 (Kemp, 2019). Moreover, these platforms expanded into applications and smartphones, becoming deeply embedded into people's daily lives (Burgess *et al.*, 2018). Although debates over the transition to Web 3.0 continue (Allen, 2013; Rudman and Bruwer, 2016), this research remains focused on Web 2.0 and the role of SMPs in digital governance.

Following the above overview of its emergence, I now review scholarly descriptions of SMPs, noting that there is no standard accepted definition. From technical-business perspectives, Kaplan and Haenlein (2010, p. 61) describe SMPs as 'a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content'. Others, such as Poell *et al.* (2019, p. 3) define platforms as '(re)programmable digital infrastructures that facilitate and shape personalised interactions among end-users and complementors, organised through the systematic collection, algorithmic processing, monetisation, and circulation of data'. While these definitions focus on structural and infrastructural dimensions of SMPs, other scholars approach them through communication and interaction lenses. From this perspective, Carr and Hayes (2015, p. 50) define SMPs as:

Social media are Internet-based channels that allow users to opportunistically interact and selectively represent, either in real-time or asynchronously, with both broad audiences who derive value from user-generated content and the perception of interaction with others.

They offer a user-centric definition by highlighting the interactive nature of platforms. This aligns with scholars who characterised Web 2.0's interactivity as inherently democratic (like Cormode and Krishnamurthy, 2008). Taken together,

these diverse definitions demonstrate SMPs' operation at the intersection of technology, communication, and governance, highlighting the need to analyse them holistically rather than as a single disciplinary framework.

There were two reasons why my research focused on SMPs. One was because SMPs have extensive user reach globally, which also feeds into a capital-driven business model. In 2019, 3.48 billion out of 4.3 billion internet users (81%) used social media (Kemp, 2019). These numbers help explain why some scholars understand SMPs not only as tools of communication but also as capitalist enterprises (Andrejevic, 2011; Fuchs, 2024). Fuchs (2024) argues that SMPs operate through capital accumulation where they exploit users through data and unpaid labour. He suggests that these dynamics contribute to global digital divides (Fuchs, 2024). Similarly, Andrejevic (2011) views SMPs as a commercial model of surveillance in which user data is commodified and the digital labour they put in is alienated. These political economic arguments can be complemented with an interdisciplinary critique from Vaidhyanathan (2018), who argues that analyses focused only on exploitation and capital accumulation overlook how platforms reshape cultural practices, regulatory debates, and public life. While underscoring the remaining importance, his critique reminds us of the multi-dimensional and interdisciplinary lenses needed when examining SMPs.

Another reason why I focused on SMPs is because they have evolved beyond social networking channels and become key political tools. They not only facilitate freedom of speech and access to information for users, but are also used by governments, institutions, and political leaders to engage in 'public-private interaction' (Torfing *et al.*, 2020, p. 94). Thus, scholars argue that SMPs are not neutral, but in fact influence individual interactions and 'institutional structures and professional routines' (van Dijck and Poell, 2013, pp. 3-5). The incidents mentioned in Subsection 1.2.1 demonstrate the politicisation of SMPs, showing that they are central to understanding how democracies regulate, control, and engage with these platforms.

In summary, SMPs' extensive reach, business model, and their political significance makes them a valuable medium through which to study digital

governance in democracies. Their capacity to be used for both democratic and authoritarian purposes, power to impact on real life, and lack of neutrality reveals their dual usability, as discussed next.

1.2.3 What are Dual-use Technologies and Why do They Matter?

Dual-use technologies have been on the international political agenda since the 1950s due to the use of nuclear weapons and developments in nuclear energy (Oltmann, 2015; Miller, 2018; Riecke, 2023). Although there is no single definition of dual-use technologies, they are generally understood to be technologies which can be used for both civilian and military purposes (Oltmann, 2015; Miller, 2018; Riebe and Reuter, 2019; Riecke, 2023). Considering the change in political agenda and increased uncertainties in the 21st century following the 9/11 terror attacks, some scholars have pointed out the need to redefine dual-use technologies, especially in the cybersphere (Riecke, 2023). They have started to re-define dual-use as ‘beneficial and harmful’ (Miller, 2018, p. 6; Riebe and Reuter, 2019, p. 170), ‘good and bad’, or ‘benevolent and malevolent’ (Oltmann, 2015, p. 327). However, this has created a dichotomy, where some scholars have remained in the traditional realm to study ‘dual use’ through the ‘WMD-affect²’ (Miller, 2018), whilst others have interpreted and included SMPs in the term dual-use by pointing out their civilian and military uses (Baseggio *et al.*, 2020) or their good and bad uses (Lipschultz, 2022).

Previous studies on dual-use has largely concentrated on the life and engineering sciences (Oltmann, 2015). My research aimed to fill this gap by focusing on dual-use technologies and operations on SMPs through interdisciplinary lenses. I explain two ways in which my research examines SMPs’ dual usability within its scope. The first way is through users’ online engagement and communications on SMPs, from which platforms make profit (see Subsection 1.2.2 for the user-centric definition and political economy of SMPs). Lindgren (2022) calls this contradictory nature of SMPs ‘double edged’. I expand on both the user and platform sides of such dual usability below.

² ‘WMD’ stands for ‘weapons of mass destruction’.

In relation to users, SMPs provide different functions, especially in differing political contexts. Some scholars see SMPs as a form of civic engagement and participation in democratic contexts (Wessels, 2018; Edwards *et al.*, 2021). In non-democratic contexts, SMPs are seen as a tool that enabled protestors to communicate, coordinate, and report information during events like the Arab Spring, which resulted in overthrowing governments in Tunisia, Yemen, Egypt, and Libya (Bebawi and Bossio, 2014; Deibert, 2015; Aal *et al.*, 2019). While these uses reflect SMPs' liberatory potential (Diamond, 2010), the Tunisian government's arrest of SMP users for their online activities exemplified an authoritarian response aimed at controlling citizens (Deibert, 2015, p. 67). Some scholars view this from the ecology of war online, where users not only engage in trending topics but also with war content in a company-controlled sphere (Ford and Hoskins, 2022). Others extend Noelle-Neumann's (1974) spiral of silence theory, arguing that users often refrain from expressing minority opinions due to perceived social pressure online (Gearhart and Zhang, 2015). These examples not only illustrate SMPs' dual usability for users, but also reveal varied ways users engage with SMPs, like active participation or strategic silence.

In relation to platforms, the literature highlights the potential for computational propaganda in SMPs. Woolley and Howard (2018) analyse SMP-caused misinformation and manipulation through various forms of coordinated inauthentic behaviour, including algorithms, surveillance, bots, hate speech, and junk news. These practices have become increasingly integrated into social, political, and military operations in countries that are democratic. Woolley and Howard (2018, p. 5) describe this as a form of warfare where 'the goal is to manipulate information online in order to change people's opinions and, ultimately, behaviour'. This reveals SMPs' dual usability, as they are referred to not only as technological infrastructures for communication, but also as instruments of influence and control in the digital sphere.

The second way I explain SMPs' dual usability in my research is by exploring the external operations employed on them. SMPs have become avenues where dual-use technologies can be employed for actions like data collection and discourse shaping to protect a regime (Gunitsky, 2015). Thus, these operations differ from inbuilt features or actions of the platforms, but rather refer to externally

employed tools, such as spywares, bots, and targeted advertisements. These practices and technologies are evident not only in authoritarian regimes (see Chapter 2), but also in democracies, highlighting digital dual-use operations as a global concern. One example of this is content moderation. Previous research has shown concerning effects of content moderation on freedom of speech (Etlinger, 2019; Edwards *et al.*, 2021), highlighting that online censorship rose 5.6% globally between 2011 and 2018 (Chang and Lin, 2020, p. 880). This demonstrates how SMPs serve not only as communicative structures for users, but also as operational terrains for other technology operators and governments, complicating their roles in digital governance.

Following my two distinct explanations of dual usability in SMPs, I used the theory of affordances to contextualise dual-use mechanisms in my research. Originally developed by Gibson in 1970s, affordances refer to the possibilities that an environment or object offers: ‘the affordances of the environment are what it offers the animal, what it provides or furnishes, either for good or ill’ (Gibson, 2015, p. 119). Gibson (2015) argues that the values and meanings of things in the environment can be directly perceived, and that different objects mean different affordances depending on the actor. In extending this concept to technologies, Hutchby (2001) offers a ‘third way’ to existing constructivists and realists, suggesting that technologies possess affordances that both shape and are shaped by human practices. Like Gibson, he emphasises that ‘different technologies possess different affordances’ and that these affordances can have different meanings for different species (Hutchby, 2001, pp. 447-448). In relation to social networking sites³, Boyd (2010, pp. 53-66) discusses how ‘bits’ play a role in the architecture of networked technologies, which creates affordances, influencing the dynamics of the sphere where networked publics participate. Together, these perspectives help explain how dual-use technologies may offer different affordances to governments, corporations, or individual users, as I ascertained during my research. Using theory of affordances enabled me to make a context-based examination of SMPs’ dual usability and the dual-use operations employed within them.

³ Social networking sites are digital platforms of interactions. They are categories within social media platforms.

Taken together, the three questions set out in this section explain the purpose and importance of my research - to explore democracies' digital governance through SMPs, while considering their contradictory nature, dual-use affordances, real-world implications, and states' approaches in governing them.

1.3 Research Aim and Objectives

Considering non-democratic digital incidents observed in democracies (see Subsection 1.2.1), my research challenged the prevailing Western-centric view of digital governance (see Chapter 2). By acknowledging possible reflexive changes that might have occurred at micro, meso, and macro levels following incidents like the Cambridge Analytica scandal (O'Loughlin, 2020), this study adopted an inductive approach to gain a deeper understanding of democracies' digital governance of SMPs. My central research aim was to explore the dual-use operations, government actions, existing technologies, laws, individual rights, and socio-political implications of SMPs in order to understand how democracies have constructed their digital governance. To achieve this, my research employed a comparative case study design and developed a qualitatively driven multimethod approach. Combining both quantitative and qualitative data, it examined India and the UK's digital governance, with a specific focus on Facebook and Twitter.

Based on the explanations given regarding my research purpose (Section 1.2) and the gap identified in the literature (see Chapter 2), I generated three sets of sub-research questions (SRQs) to help address my main research questions:

Main research questions: How do India and the UK construct their digital governance in relation to social media platforms? What is the broader significance of this for democracies and digital governance?

SRQ.1 What are the existing digital dual-use operations involving social media platforms in India and the UK? Who conducts these operations?

SRQ.2 How do legal frameworks inform the regulation of digital dual-use operations and stakeholders? What legal concerns are raised regarding the digital governance of social media platforms?

SRQ.3 What implications and concerns do experts raise regarding the digital governance of social media platforms and their impact on the public in India and the UK?

To operationalise these questions, I developed three research objectives. These objectives were structured around the core aim of understanding how India and the UK construct their digital governance of SMPs.

First, this study analysed existing digital dual-use operations in India and the UK to understand how they integrated operations that can be both beneficial and harmful. This not only provided a socio-political context to operations involving SMPs, but also identified actors in their digital spheres and illustrated the way technology was being interpreted in each country.

Second, I focused on understanding how Indian and UK democracies protected individual rights and regulated stakeholders and technologies. This required analysing their legal frameworks in relation to human rights, state legislation, government documents and regulatory operations, as well as identifying legal concerns in both countries.

Third, I explored broader implications of digital governance for the public through opinions and observations of experts in both countries (see Chapter 5 for methodological details). To validate these primary insights, I expanded this interview data with secondary data and public opinion data when necessary.

Through these objectives, this study empirically examined the dynamic construction of digital governance through digital dual-use technology (SRQ.1), legal frameworks (SRQ.2), and societal influence (SRQ.3), following a digital structuration framework (see Chapter 4). Through this way, my study ascertained how the Indian and UK democracies have constructed their digital governance in relation to SMPs.

1.4 Key Contributions of the Thesis

My thesis makes four key contributions to studies on the digital governance of SMPs: theoretical, methodological, empirical, and conceptual.

First, I developed a structuration-based theoretical framework for understanding digital governance. By focusing on the triadic relationship between structure, agency, and technology, this framework offers a new lens through which to understand the dynamic construction and shaping of digital governance of social media platforms across different contexts.

Second, I used a qualitatively driven multimethod approach for my comparative case study research. It consisted of three sequential stages of data collection, which not only captured data from diverse sources but also refined the scope of my research. Through an inductive approach, I generated three themes: -veillance, content control, and shaped discourse. Each theme was defined and substantiated with coding tables, offering a novel methodological model for my study. Importantly, this data-driven definition distinguished my themes from the existing literature, like Mann's (2013) -veillance plane and the generally accepted analytical studies on 'discourse', offering an original thematic contribution to empirical studies.

Third, my thesis provides an empirical contribution, as I analysed real-world data on the digital governance of social media platforms in India and the UK. It explores digital dual-use operations, legal frameworks, and the observed implications on the public, demonstrating how digital governance is constructed and dynamically shaped in different national contexts.

Fourth, my research findings propose the concept of digital hybrid regimes. Building on the literature of hybrid regimes and following Gilbert and Mohseni's (2011) approach, I have defined digital hybrid regimes as a distinct form of digital governance that is separate from digital democracy and digital authoritarianism. This conceptual contribution addresses the gap identified in the literature (see Chapter 2) and advances interdisciplinary scholarship on digital governance.

Together, these four contributions demonstrate the originality and interdisciplinary significance of my research.

1.5 Thesis Structure

This thesis consists of ten chapters. Following this introduction, Chapter 2 presents a literature review of digital governance, while Chapter 3 provides context on India and the UK. Chapter 4 describes my innovative analytical framework, followed by the research design and methodology in Chapter 5. Chapters 6 to 8 discuss my findings on India and the UK. Chapter 9 compares these findings, addressing each SRQ and then articulating the answer to my main research questions, which informs my conceptual contribution on digital hybrid regimes. Finally, Chapter 10 develops this contribution and concludes the thesis with my research reflections.

Chapter 2 Literature Review

This chapter reports the literature review undertaken on digital governance in democratic and authoritarian regimes. Although the term governance originates from the ancient Greek word ‘kubernao’ (Mollah, 2019), which means to steer, one of its systematic definitions in the modern political system was given by the World Bank: ‘governance is defined as the manner in which power is exercised in the management of a country’s economic and social resources for development’ (World Bank, 1992, p. 1). Thus, governance is not a determinant of what regime a state practices, but is about a ‘government’s ability to make and enforce rules, and to deliver services, regardless of whether that government is democratic or not’ (Fukuyama, 2013, p. 350), which differs from the deterritorial, multi-stakeholder, and uncertainty aspects of cyberspace in which digital governance takes place (Medeiros and Goldoni, 2020).

Digital governance differs from state governance as it operates within the cybersphere, which is ‘not constrained by territorial boundaries or border controls’, but is an immaterial virtual space (Medeiros and Goldoni, 2020, p. 37). The literature is dominated by and often confuses internet governance with digital governance. In fact, these are two different things. Internet governance is the management and regulation of a global infrastructure that involves multiple stakeholders, including governments, businesses, and civil society groups (Flyverbom *et al.*, 2019). In contrast, digital governance is a broader concept which includes not just internet governance, but also the regulation and management of digital technologies and their impact on society (Komaitis and Carter, 2023). Thus, the notion of digital governance encompasses not only the internet and other multi-stakeholders in the borderless cybersphere but also differentiates it from state governance.

Although digital governance by states was pioneered by a democratic country, the US, where the internet was invented and first publicised (Chadwick, 2006), it has proliferated to other regimes over time. This chapter reviews the literature on key features, practices, and ideological underpinnings of digital governance within two opposing regimes. The first section reviews the literature on democracy and digital democracy, while the second section covers

authoritarianism and digital authoritarianism. The third section provides a discussion on these two regimes and concludes by highlighting the gap that my research sought to fill.

2.1 Democracy

Democracy is one of the oldest and most popular forms of governance. Rooted in Ancient Greece, it comes from the word '*demokratia*' (Hanson, 1989, p. 71 as cited in Dahl, 2000; Held, 2006; Young, 2023), which means 'people rule' (Held, 2006; Young, 2023). Democracy has evolved over the years (Young, 2023); there is no single form of democracy in the modern political system (Held, 2006; Hobson, 2015; Wright, 2019). According to Held (2006), types of democracies have diversified due to the different values societies attribute to words like rule, authority, and people, which can be further discussed through global political shifts.

The outcomes of the two World Wars and the subsequent Cold War were viewed as a global victory for democracy in the late 1980s (Fukuyama, 1989), as the number of democracies increased worldwide (Huntington, 1991). However, the literature from the early 2000s onwards shows that the power of democracies started getting disrupted and weakened across the world. Some scholars viewed this as a result of newly formed states' incomplete transition to democracy (Merkel, 2004; Schmotz, 2019). Merkel (2004), for instance, called these 'defective democracies'⁴. This described a situation where minimal democratic conditions like elections existed, but alongside maximal diminishment of democratic principles, including 'systematic deficiencies regarding civil rights, horizontal control, political participation, and the effective power to govern' (Schmotz, 2019, p. 522). Despite these changes, it is essential to identify some core characteristics of democracies before examining the literature on digital democracies.

According to Schmitter and Karl (1991, p. 76) democracy is a 'regime or system of governance' which has a ruler who can be held accountable for their actions,

⁴ Such as illiberal democracy, delegative democracy, exclusive democracy, and domain democracy (Schmotz, 2019, p. 522; Merkel, 2004).

citizens are equal, and the focus is on the public realm. It fosters political competition and fair elections, upholding majority rule (Schmitter and Karl, 1991). However, a democracy's effectiveness depends on adherence to 'the "rule of law" regarding its own procedures', and respect for rights (Schmitter and Karl, 1991, p. 81), emphasising that democracy extends beyond formal structures to actual practice. This can be expanded with two democratic principles from Dahl (2000)'s ten advantages⁵. First is a guarantee of individuals' fundamental rights. Dahl (2000, p. 48) asserts that 'rights are among the building blocks of a democratic process of a government', thus, should not merely exist in written law, but should be practiced in democracies. Second, democracy provides certain freedoms to individuals, including the right to practice religion, and the right to express opinions on political matters (Dahl, 2000). These principles underscore democracy's commitment to individual rights and freedoms as essential civic elements.

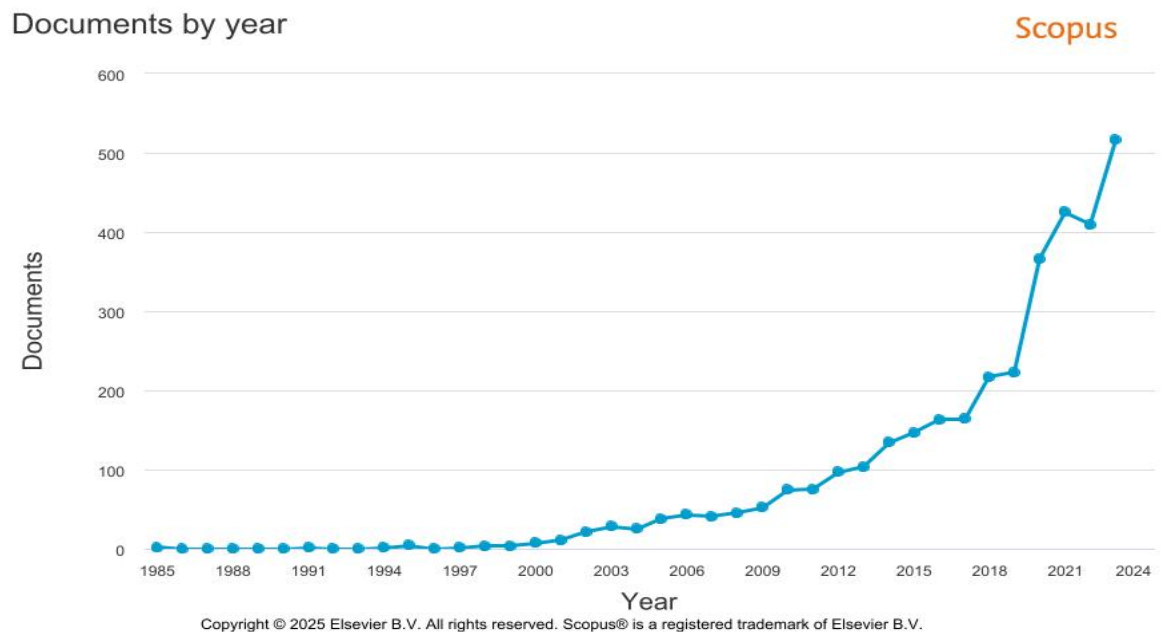
2.1.1 Digital Democracy

Considering the development and increasing significance of digital democracy, I carried out a keyword search on 'digital AND democracy' on Scopus, as shown in Figure 2.1. Thus, my literature review on digital democracy focuses from 1985 to 2023⁶. I chose this period because it captures both the emergence and the expansion of academic research on digital democracy.

⁵ Democracy procedures' desirable consequences: (1) Avoid tyranny, (2) Essential rights, (3) General freedom, (4) Self-determination, (5) Moral autonomy, (6) Human development, (7) Protecting essential personal interests, (8) Political equality; in addition, modern democracies produce: (9) Peace-seeking, and (10) Prosperity (Dahl, 2000, p. 45).

⁶ My analysis covered 1985 to 2023 (the year when I conducted this analysis), but the graph created on Scopus shows 2024 by default (same applies for digital authoritarianism).

Figure 2.1: Scopus (2023b) search on ‘digital AND democracy’



The literature on digital democracy goes back to the late 20th century. Early scholars showed a clear appreciation of emerging technologies in democracies and believed that they might strengthen democracies. Dahl (1989, pp. 338-9) discussed how ‘virtual telecommunications’ could help democracies reduce the knowledge gap between elites and ordinary citizens by making information available to all and increasing political participation. The popular press echoed this optimism; Clift (1998) claimed that the ‘Internet will save democracy’ by making information accessible to citizens, requiring various media outlets to inform the public, increase advocacy, foster the development of information and communication technologies (ICTs), and enable online civic participation.

In the 1990s, digital democracy was often discussed in relation to state governance, public engagement, and technological developments on the internet. During this phase, democracy was conceptualised in several ways, including as ‘electronic democracy’ or ‘teledemocracy’ (Berg and Hoffman, 2021), and ‘cyber democracy’ (Hague and Loader, 1999). Hague and Loader (1999, p. 3) described digital democracy as ‘bringing together existing electronic technologies through developments in digital data transfer that unleashes the potential of ICTs’. They defined its characteristics as including ‘interactivity, global network, free speech, free association, construction and dissemination of

information, challenge to professional and official perspectives, and breakdown of nation-state identity' (Hague and Loader, 1999). Instead of viewing technology as a solution to democratic challenges (like Dahl 1989 and Clift 1998 above), Hague and Loader (1999) saw it as a transformation of democracy into digital forms, positing that the digital 'demos' would transfer power to the people. This change was also seen in technologically leading countries, like the US, integrating digital governance onto their agenda. For instance, the first digital administrative programme the US created was under the National Performance Review from 1993 to the late 1990s (Chadwick, 2006), which illustrates a democratic state beginning to territorialise cyberspace.

In the early 2000s, the proliferation of the internet became more apparent in governments' frameworks and public participation. The US President Bill Clinton's administration established the first government portal for citizens to access information and services, 'firstgov' (Chadwick, 2006, p. 180). While this period marked early developments in states' adaptations to the digital, it also witnessed an increase in political participation. Some scholars viewed digital democracy as the use of technology to 'increase political democracy or the participation of citizens in democratic communication' (van Dijk and Hacker, 2000, p. 1). Studies have found that access to the internet had a positive impact on voter turnout in the 2000 US elections (Tolbert and McNeal, 2003).

By 2010, digital democracy had reached its peak, when Hillary Clinton gave a speech calling for advancing democracy and freedom on the internet (MacKinnon, 2011; Polyakova and Meserole, 2019), while criticising the Chinese decision to ban Google, touching on restrictions on freedom of expression and related punishments in the Middle East, and countries breaching privacy (Clinton, 2010). However, that same year, the US's digital democratic image was damaged when Wikileaks shared confidential state documents with the public. Under the guise of transparent journalism or 'truth telling' to fix problems within democracies (Wikileaks, n.d.), Wikileaks disseminated videos about the US war in Iraq and Afghanistan, including footage showing civilians being killed by US officials (Roberts, 2012; Whittaker, 2018), breaking the digital democratic reputation the country had held at the start of the year.

The Wikileaks incident was followed by Edward Snowden's revelations in 2013. Snowden, a former intelligence officer who had worked for the US National Security Agency (NSA) through a private technology company, exposed secret operations called PRISM in the US and Tempora in the UK, where the respective countries conducted surveillance and collected data from big tech companies (MacAskill and Dance, 2013). These revelations increased concerns, raised many questions, and heightened public awareness about the technological tools being used by governments (Flyverbom *et al.*, 2019). In response, US President Barack Obama gave a speech that justified these practices as necessary, stating: 'But I think it's important to recognise that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience. We're going to have to make some choices as a society' (Obama, 2013). Although this exemplifies a speech act for justifying operations under national security (see the theory of securitisation in Subsection 1.2.1), scholars argue that the Snowden revelations did reduce levels of trust between the state and its citizens (van Dijck, 2014; Sørensen *et al.*, 2020).

Following these incidents, technology started to be seen as a commodity for private companies, leading to discussions on digital capitalism (Sadowski, 2020, as cited in Zuboff, 2019; Stubbs, 2023). This shifted digital democracies towards a profit-oriented adaptation and use of the digital sphere, overshadowing its democratic potential. For instance, Cambridge Analytica, a British data analytics firm, operated targeted personal advertisements during both the US presidential elections and the UK referendum on leaving the EU ('Brexit') in 2016. By using specific wording of terms and conditions in an application called 'thisisyourdigitallife', users unwittingly agreed not only to share their personal data, but also allowed Facebook to collect their friends' data, resulting in millions of profile data being harvested and then used for targeted political advertisements (Cadwalladr and Graham-Harrison, 2018). Frances Haugen, a whistleblower who worked at Facebook, has shared documents about the company's interference in elections, data collection and sharing, promotion of misinformation, and hate speech, among other misuses (Paul and Milmo, 2021). This not only raised questions about free and fair elections in democracies but also exposed the use of digital political manipulation within them.

In summary, this literature review of the evolution of digital democracy highlights a gap between early theoretical optimism and practical realities over time. While initially seen as a tool for greater participation, its governance has shifted from governments to the private sector, raising concerns over undemocratic implications, data misuse, and digital authoritarian risks within democracies themselves.

2.2 Authoritarianism

Authoritarianism is one of the non-democratic forms of governance often associated with dictatorial regimes such as totalitarianism and autocracy (Svolik, 2012). It is a centralised form of governance that is socio-politically shaped and adapted by states. There are various forms of authoritarianism, including sultanist, personalist, military, single-party, bureaucratic-military, organic statist, among others listed in the literature (Linz, 2000; Svolik, 2012). Despite these variations, scholars viewed the period following the 1990s as a crisis for authoritarian regimes due to the third wave of democratisation (Pye, 1990; Schmotz, 2019; Wright, 2019). According to Pye (1990), this crisis increased the decentralisation of power and increase in pluralism across authoritarian governments, compelling them to lose some of their key features and adopt some liberal practices, leading to debates on hybrid regimes.

Some scholars viewed hybrid regimes as transitional, moving towards democratisation. One type of such a hybrid regime is called competitive authoritarianism. This is where a state has fraudulent elections, a dependent legislature and judiciary, and state pressured media (Levitsky and Way, 2002). Another type of hybrid regime examined in the literature is through elections. Diamond (2002) referred to authoritarian regimes with multi-party elections as electoral authoritarianism, where the level of their authoritarianism varied based on 'freedom' and 'fairness' during elections. Unlike Diamond, Brownlee (2007, pp. 3-9) argued that elections in authoritarian regimes do not guarantee democracy but instead indicate a regime's adaptation to global trends, because elections in those hybrid states were questionable, like Egypt and Malaysia, and only a slight change was observed in Iran and the Philippines. Despite their different perspectives and points raised, all these scholars underscored the role

elections play in authoritarian regimes' debates about becoming hybrid. Indeed, some scholars argue that having such hybrid features help authoritarians to survive and protect their regimes (Geddes, 2000, as cited in Chang and Golden, 2010) and resist democratic demands from society, since they are structurally constructed as democratic, albeit authoritarian in practice (Brancati, 2014).

Instead of approaching hybrid regimes as having democratic features or limited authoritarianism, Gilbert and Mohseni (2011) conceptualised them as a distinct form of governance that is neither democratic nor authoritarian. They argued that the confusion in the literature stems from applying democratic features like elections and multi-party systems to states with authoritarian practices (Gilbert and Mohseni, 2011). Focusing on hybrid regimes between 1990 to 2000, they re-assessed hybrid regimes and devised three types: 'illiberal hybrid regime', 'illiberal tutelary hybrid regime', and 'tutelary hybrid regime' (Gilbert and Mohseni, 2011, pp. 290-2). This not only contributes to the recognition of a distinct hybrid state-governance type but also demonstrates its diversity by highlighting that there is no single type of hybrid regime either. Given this distinction between hybrid and authoritarian regimes, it is important to outline the key characteristics of authoritarianism before presenting my literature review on digital authoritarianism.

Authoritarianism is a top-down form of rule that ignores popular consent and limits the public, with 'claims of authority over individual liberty' (Wright, 2019, p. 22). The power of an authoritarian government is not centred on a single leader, but on a larger group who share 'background, ideology, or interests' (Brownlee, 2007, p. 12). Some scholars highlight the importance of forming government institutions in authoritarian regimes, arguing that their independency might endanger the regime's survival, while their absence can undermine the functioning of an authoritarian government (Svolik, 2012, p. 20). Although institutionalisation is a democratic character within an authoritarian system, some scholars argue that examining institutions can be seen as a way to study and understand political actors' behaviours and their effectiveness in authoritarian regimes (Brownlee, 2007, p. 10). This includes the role of 'military involvement, restrictions on political parties, legislative selections, and executive selections' (Svolik, 2012, p. 32), which configure different types of

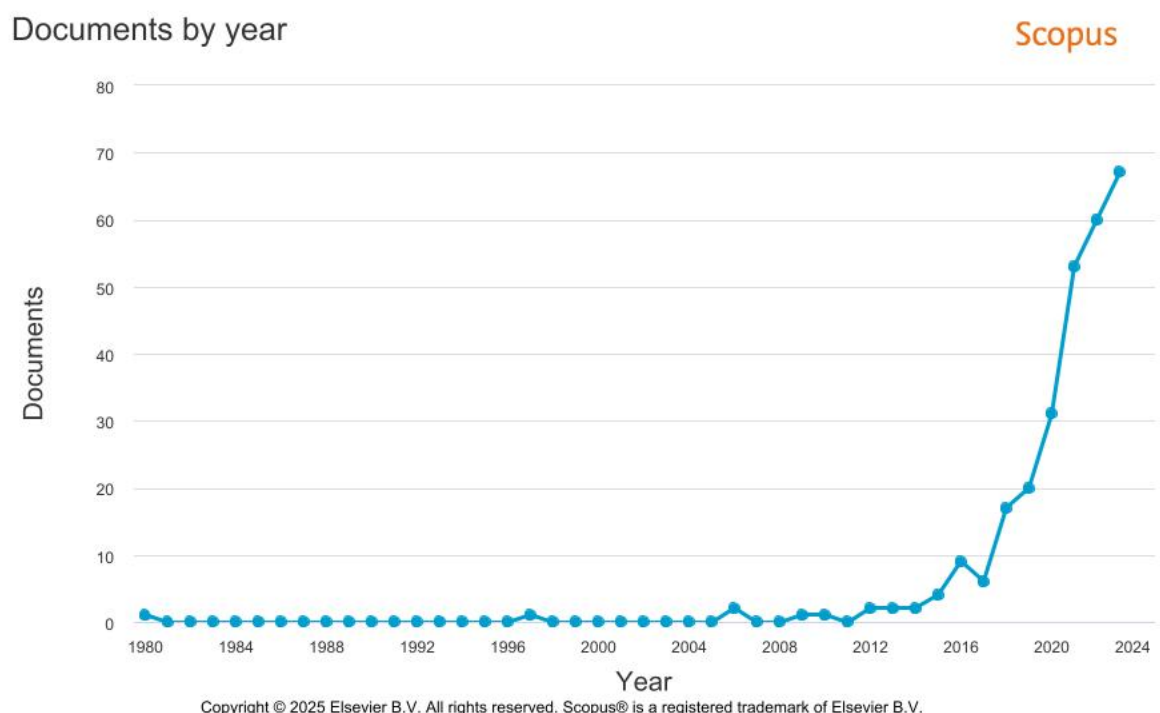
authoritarian regimes. In spite of these differences between authoritarian types, some highlight their primary goal as focusing on their own stability and survivability (Svolik, 2012).

Having provided a brief introduction on authoritarian governance and its key features, the next subsection details my review of digital authoritarianism literature.

2.2.1 Digital Authoritarianism

To ensure that my literature review on digital authoritarianism focused on a relevant period, I conducted a keyword search for ‘digital AND authoritarianism’ on Scopus. As Figure 2.2 shows, I review the literature from the 1980s to 2023⁷. Similar to my explanation in Subsection 2.1.1, I chose this period to capture the early debates and the later evolution of digital authoritarianism in the scholarship.

Figure 2.2: Scopus (2023a) search on ‘digital AND authoritarianism’



Some scholars thought that the internet and ICTs would reduce the power of authoritarian governments. For instance, Pye (1990, p. 9) argued that the

⁷ The analysis dates ranged from 1980 to 2023 (2023 is the year when I conducted my analysis), but Scopus results show 2024 by default.

technological revolution would challenge the centralisation of power in authoritarian regimes. However, challenging early views that the internet and other emerging ICTs were democratic, transnational, and borderless, authoritarians have found ways to establish control online (MacKinnon, 2011; Deibert, 2015).

There is no single definition of digital authoritarianism. Howells and Henry (2021, p. 2) define it as a type of internet governance ‘in which digital authoritarians can exercise censorship, surveillance, and manipulation in relation to the internet infrastructure and stakeholders who rely on it’. In contrast, Yayboke and Brannen (2020, p. 2) define digital authoritarianism ‘as the use of the Internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties’. Their definition is unique as it retains the possibility that illiberal democracies may also have authoritarian tendencies online.

Different digital authoritarian countries featured in the literature, like China, Russia, and Iran. China was one of the first digital authoritarian countries to build its own digital infrastructure, with centralised state governance. Russia illustrates a mixture of digital authoritarianism (Polyakova and Meserole, 2019; Howells and Henry, 2021) and digital hybrid forms, due to its formal democratic state governance (Wright, 2019)⁸. It focuses its digital governance on protecting state interest from the West online, with President Putin calling the internet a ‘CIA Project’ (MacAskill, 2014; Polyakova and Meserole, 2019). Iran’s digital authoritarianism emerged primarily following the 2009 election protests (also known as the Green Movement), and it focuses on protecting regime and religious values online (Diamond, 2010; Michaelsen, 2018a; Michaelsen, 2018b). Despite their differences, the literature highlights some digital authoritarian characteristics encompassing technology and the law as part of their governance.

⁸ Wright (2019, p.31) categorises China as digital authoritarian, the US as a digital liberal democracy, and Russia as a digital hybrid regime.

From my analysis of the literature, I have identified four technology-related aspects of digital authoritarianism: i) surveillance and data collection, ii) censorship, iii) manipulation, and iv) cyber-attacks. First, a vast amount of literature agrees that surveillance is a key part of digital authoritarianism (MacKinnon, 2011; Wright, 2019; Chang and Lin, 2020; Howells and Henry, 2021; Brandt, 2022). One of the primary reasons for this, scholars argue, is that surveillance ensures a regime's legitimacy online (MacKinnon, 2011; Chang and Lin, 2020; Howells and Henry, 2021). However, the literature shows that states have different ways of adopting surveillance as part of their digital authoritarian governance. For instance, China has the Golden Shield Project, the first phase of which is dedicated to 'building a national database, monitor the Internet and track IP systems', while the second phase is on 'placing of surveillance cameras in the streets' (Xu, 2020). It works on data localisation (MacKinnon, 2011; Liu, 2020), which is viewed as a way to protect China from international threats and secure its long-term economic and technological advancement (Liu, 2020). This is one of the reasons why the Chinese government is incorporated with more than 150 firms, including Alibaba and Baidu (CCTV, 2016, as cited in Liang *et al.*, 2018).

Russia has a legally binding monitoring and data collection operation, its System of Operative Investigative Measures (SORM). SORM allows surveillance cameras to be placed in Russian cities and legally requires Internet Service Providers (ISPs) and telecom providers to give the government access to their data as well as sharing copies of data with the government through an installed 'black box' (Morgus, 2019; Polyakova and Meserole, 2019). Thus, SORM is a mixture of surveillance and dataveillance which allows the government to process data in several ways, including decryption by the Federal Security Service (Morgus, 2019).

The literature review revealed two methods of surveillance methods in Iran. One method is known as lateral surveillance, which is non-technical and carried out by the Revolutionary Guards cybercrime unit. These groups monitor Facebook activities and, depending on the content, the government arrests users opposing the regime (Centre for Human Rights in Iran, 2015, as cited in Michaelsen, 2017, p. 467). Another method is targeted surveillance on activists (Michaelsen,

2018b), not only at the domestic level, but also internationally (Michaelsen, 2017), which explains why Iran is one of the biggest importers of surveillance and web monitoring devices manufactured by Western companies (Citizen lab, 2013, as cited in Michaelsen, 2017). In this way, rather than performing mass-scale surveillance like China or Russia, Iran's digital authoritarianism illustrates targeted surveillance.

The second aspect I identified in the literature is controlling information in a way that benefits digital authoritarians (Diamond, 2010; Deibert, 2015). Such control is achieved via filtering (Chang and Lin, 2020; Kawerau *et al.*, 2023), content removal requests (Diamond, 2010; Erixon and Lee-Makiyama, 2011), blocking (MacKinnon, 2011; Kawerau *et al.*, 2023), banning platforms or websites (Weber, 2017; Michaelsen, 2018b), 'shut[ting] down particular servers' (MacKinnon, 2011; Kawerau *et al.*, 2023), internet shutdowns (Deibert, 2010, as cited in Jiang, 2010, p. 75), and limiting access to information (Yayboke and Brannen, 2020). Some scholars consider this method as a way to shape society (Chang and Lin, 2020), control ideology (Michaelsen, 2017), control social and political stability (Erixon and Lee-Makiyama, 2011), and maintain a regime's legitimacy (Howells and Henry, 2021). As these comprise diverse tools used to help digital authoritarian governance, it is important to grasp their context through the examples given in the literature.

For instance, China has a nationwide operation to control all content that leaves and enters the country, the Great Firewall of China (referred to as the Firewall). The Firewall allows strict regulation of ISPs, polices the internet, and conducts content control and censorship operations (Diamond, 2010; Howells and Henry, 2021). As a result of its mass controls, the Firewall has banned some international platforms in China, such as Google, Facebook and Twitter (Diamond, 2010; Howells and Henry, 2021). Another example is Iran's national intelligence filtering project, known as the 'Halal Internet' (RSF_en, 2016). This aims to protect Iran's national security and religious morality from Western influence and content (Michaelsen, 2018b). The 'Halal Internet' has resulted in websites and social media platforms being banned, arrests, mandatory ID registration, and restricted online access (RSF_en, 2016). Moreover, Iran's Telecommunications Corporation has purchased a censorship tool from China's

ZTE Corporation (Chang and Lin, 2020). Like surveillance, this illustrates Iran's reliance on the international technology market in its digital authoritarian governance.

The third aspect I identified in digital authoritarian literature is manipulating and shaping discourse, which varies between states. Although China's digital authoritarianism is predominantly carried out through technological tools, information manipulation is another one of its main digital authoritarian methods. This involves using voluntary or paid users (MacKinnon, 2011; Shahbaz, 2018) called '50-centers', who post online in support of the state and report negative comments (Diamond, 2010, p. 74; Bulovsky, 2019). In comparison, Russia relies less on censorship (Howells and Henry, 2021), but has pioneered information manipulation (Morgus, 2019; Wright, 2019), including social and electoral manipulation through misinformation and disinformation (Morgus, 2019; Yayboke and Brannen, 2020). It is also important to note that Russia's campaigns on social media focus not only on domestic audiences, but also internationally (Krekó, 2021; Brandt, 2022). Hence, Russia's manipulation abroad has created uncertainty about security versus information control (Morgus, 2019) and weakened people's trust in UK, EU, and US institutions (Yayboke and Brannen, 2020).

The last aspect I identified in the literature is cyber-attacks. Unlike the above, cyber-attacks are a more targeted method of operations. For instance, China quashes critical voices not only through technologies and partnering with private firms, but also via targeted cyber-attacks on journalists (CCTV, 2016, as cited in Liang *et al.*, 2018). Another prevailing example in the literature is Iran's use of cyber-attacks, such as phishing and hacking. Michaelsen (2018a)'s study identified different types of targeted attacks experienced by activists who fled Iran, including large-scale attacks on those who criticised the regime, hacking journalists and activists' ICT devices, sending personalised malicious links or fake telephone conversations to either gain access to their digital information. These underscore the transnational nature of the digital sphere and shows how Iran uses it for the regime's benefit.

These four technology-related aspects highlight how technologies aid digital authoritarianism, while also leading to a problem of proliferation across states (Polyakova and Meserole, 2019; Howells and Henry, 2021). In their article, Polyakova and Meserole (2019) focus on digital authoritarian tools emanating from China to countries like Malaysia, Dubai, and Ethiopia, and those from Russia going to Kazakhstan, Qatar, Mexico, and Venezuela. Despite international sanctions which have prohibited ‘the government from obtaining dual-use technology for Internet filtering and surveillance’ (Mehta, 2016, as cited in Michaelsen, 2018b), the above discussion highlights Iran’s use of Chinese alternatives to Western dual-use technologies (Tansey, 2016, as cited in Michaelsen, 2018b; Chang and Lin, 2020).

Additionally, the literature demonstrates the role of laws and regulations in justifying and strengthening digital authoritarianism’s control. Scholars argue that laws help governments to justify their actions under national security concerns, which shape legal mechanisms and influence the way companies are regulated (Deibert, 2015). For instance, China’s Cyber Security Law of 2016, which has legalised data localisation (Liu, 2020), ID registration, and content control (Shahbaz, 2018). Moreover, it demands strict legal and intermediary compliance from companies and ISPs, and non-compliance may result in their work licences being revoked in China (MacKinnon, 2011; He, 2019, as cited in Polyakova and Meserole, 2019). Similarly, ISPs have a strict requirement to comply with Chinese criminal and cybersecurity law, which requires dataveillance, content removal, or user removal (FH, 2019a, pp. 6-7; Iasiello, 2017, p. 11; and Xuan, 2018, p. 72, as cited in Howells and Henry, 2021).

Likewise, Russia has a number of repressive laws as part of its digital authoritarian governance (Morgus, 2019; Polyakova and Meserole, 2019). For instance, the Yarovaya Law (2016) requires personal data to be stored for three years, and Russian officials to have access to meta data and encrypted data (ICNL, 2016, as cited in Polyakova and Meserole, 2019). Moreover, if the content shared by users does not comply with Russia’s Bloggers’ Law⁹ and the Criminal Code, which prohibits things including ‘inciting hatred’ (Article 282), ‘insulting

⁹ ‘Federal Law No. 97-FZ’ as cited in Howells and Henry, 2021, p.14.

government’ (Article 20.1), and ‘insulting the feelings of believers’ (Article 148), they may be prosecuted (Howells and Henry, 2021, p. 14). All of this illustrates the de-prioritisation of individual rights and freedoms by the law.

Different to Russia and China, Iran’s digital authoritarianism laws are influenced by moral and religious concerns as it follows Islamic Sharia Law, which helps the state to target Western values as a threat to the regime. Thus, it uses the law to support its restrictions, calling for ‘national security’ and the protection of ‘moral values’ (Article 19, 2013, as cited in Michaelsen, 2018b). For instance, Iranian trials record that Facebook and YouTube were viewed as tools of US psychological warfare and manipulation during the 2009 protests in Iran (Iran Human Rights Documentation Centre, 2010, as cited in Michaelsen, 2018b).

Scholars note the implications of digital authoritarianism. For instance, they assert that Chinese digital authoritarianism violates freedom of expression, influences public opinion, restricts political freedoms and imprisons journalists who speak out against a regime (Erixon and Lee-Makiyama, 2011), as well as weakening civil society (Chang and Lin, 2020, p. 875). Some argue that it pushes citizens to self-censor because they are surrounded by mass surveillance, prohibited from talking about political issues, and subjected to social and legal penalties (Howells and Henry, 2021). Similarly, it is argued that Russia’s legal approach enables that government to spread fear, which then leads individuals to self-censor (Weber, 2017; Morgus, 2019).

In summary, unlike Diamond’s (2010) view that technology would liberate the public (see Chapter 1), digital authoritarians have found ways to minimise risks to their regimes online. As my literature review demonstrates, their use of technology and law not only reinforces control but also underscores the dual-use nature of technology¹⁰ and the instrumental role of law in digital authoritarianism. This review has shown that, although digital authoritarian regimes share the motive ‘to maintain and expand their power’ (Michaelsen, 2018b), their approaches differ based on national contexts (Howells and Henry, 2021).

¹⁰ See Subsection 1.2.3.

2.3 Discussion: Forms of Digital Governance

My literature review findings highlighted states' transformative adaptations to digital governance from different political standpoints. Even though digital authoritarian and digital hybrid political regimes have both evolved in the same cybersphere, their use of technology, technologies' integration into politics and governance, as well the consideration of their publics show differences. To explain this argument in more detail, I discuss three key points.

The first point is the spread of democracy and the weakening of authoritarianism at state levels. From the standpoint of democratic literature, the period following the end of the two World Wars and the Cold War, and the dismantling of colonialism led to emerging new democratic states in the 1990s. The increasing number of democratic governments in the world caused most of the authoritarian regimes to lose their central powers and adopt some liberal features. Scholars who work on authoritarianism viewed this change as them becoming democratic because authoritarian governments started adopting elections (Diamond, 2002). Others saw it as an adaption to global trends in order to continue the authoritarian regimes (Brownlee, 2007). However, this literature review has shown a more nuanced understanding that some dominant authoritarian governance features were replaced with some democratic elements.

The second point is the issue of hybrid regimes resulting from the third wave of democratisation and the weakening of authoritarian governance in the 1990s. From democratic perspectives, scholars viewed hybrid regimes as states which have not completed the democratisation process but have built a governance style containing key democratic elements and some authoritarian practices (Merkel, 2004; Schmotz, 2019). In contrast, other scholars viewed hybrid regimes as being less centralised and strict than authoritarianism (Levitsky and Way, 2002), or as authoritarian regimes with liberal elections (Diamond, 2002). Others argued that the changes helped authoritarians to enhance their regimes (Brownlee, 2007; Brancati, 2014). Unlike democratic and authoritarian debates about defining hybrid regimes, Gilbert and Mohseni (2011) distinguished them

from democracies or authoritarianisms, categorising them as a unique form of governance.

The third point highlights a gap in the literature, that is the lack of appreciation that state governance may not be same as digital governance. My literature review revealed the opposing dominance of state versus digital governance regimes. The characteristics of state governance include institutions, elections, multi-party systems, and distribution of power among democratic and authoritarian states. This level of governance has a structure and hierarchical order, which varies depending on the form of governance. In contrast, digital governance takes place in a different dimensional sphere, the cybersphere, that has no territory, consists of multi-stakeholders and contains different uncertainties (Flyverbom *et al.*, 2019; Medeiros and Goldoni, 2020; Komaitis and Carter, 2023). Thus, digital governance lacks any clear governance framework like a state, comprising an ‘anarchic’ international world order with a lack of hierarchy. However, as I have explained, digital governance is not completely independent from nation states. The literature review highlighted the role played by states, especially in the ways technology is interpreted and used, and how laws and regulations are structured. Thus, this underscores the importance of state governance in understanding the digital governance context of the countries studied in my research.

In sum, I identified a research gap in the knowledge about democratic and authoritarian regimes’ digital governance in my literature review. Following the three points above, I disagree with the way the literature has categorised democracies either as digital democracies or digital authoritarianisms. Given the non-democratic outcomes of the US’s digital democracy, and scholars’ disagreement about whether Russia is a digital hybrid or authoritarian regime, my literature review findings emphasise the importance of understanding a state’s context regarding its digital governance, especially its use of technology and the law.

2.4 Conclusion

Governance, whether at a state or digital level, is socially constructed, constantly evolving and adapting to the changing world. This chapter has

discussed key features of democracies and authoritarian regimes and their digital governance forms. It has exposed a gap in the scholarly knowledge, which my research was designed to contribute to. This gap emerged from the different characteristics of state and digital-level governance. State-level governance was shown to have a stronger democratic framework, which proliferated in the 1990s and weakened authoritarian regimes that adopted democratic elements, like elections. Digital-level governance illustrated a stronger digital authoritarian character, as shown in several non-democratic incidents in the ways digital democracies have governed the digital. This nuanced observation allowed me to undertake further research in understanding democracies' digital governance. Acknowledging the role of states on digital governance, this required understanding a state's laws and regulations, the ways these are interpreted using the technology, and the resulting influence on people.

Considering the importance of national context and state-level governance raised in this chapter, the next chapter provides contextual insights into India and the UK's governance before presenting my findings on their digital governance.

Chapter 3 Contextual Insights from India and the United Kingdom

This chapter provides contextual background on the governance of India and the UK and their respective digital environments, offering a foundation for my research findings (Chapters 6 to 8). To achieve this, the chapter is divided into four sections: state and digital demographics, political system, social diversity, and a brief historical context. These sections draw on a wide range of secondary sources, including journal articles, books and websites, as well as Freedom in the World (2020-2022)¹¹ and Freedom on the Net reports (2019-2021)¹². The context provided in this chapter focuses primarily on 2019 - when I began my research - and does not extend beyond 2023, as this marked the conclusion of my data collection; therefore, it excludes any subsequent changes beyond this point.

3.1 State and Digital Demographics of India and the UK

This demographic context highlights the number of people who were governed within India and the UK. Focusing specifically on the year 2019, this context covers: state population, internet users, social media users, and most-used social media platforms (SMPs) in India and the UK.

First, India's population in 2019 was more than 1.3 billion (O'Neil, 2023), while the UK was more than 66.7 million (Park, 2020) - a clear difference at state levels, with India having almost twice as many people than the UK.

Second, the two countries' digital demographics diverged. The number of internet users in India was 644.51 million (Basuroy, 2023b), around 51% of Indians, compared to over 62 million users in the UK - 93% of its population (World Bank, n.d.). Although there was a lower percentage of internet users in India than the UK, India still had a greater number of people on the internet.

Third, since my research specifically focused on social media platforms, I discuss their demographics within the Indian and the UK contexts. In 2019, India had 310

¹¹ The reports from 2020-2022 cover the years 2019-2021.

¹² The reports cover May 2019 to May 2021.

million social media users, while this number was 45 million in the UK (Kemp, 2019). These figures highlight the number of users affected by the digital governance of SMPs in India and the UK.

Fourth, I discuss the five most popular SMPs in India and the UK, based on Statcounter's data on social media from January to December 2019. In India, these were: Facebook (88.49%), Pinterest (3.58%), YouTube (3.28%), Instagram (2.55%), and Twitter (1.83%)¹³ (Statcounter, 2024a). Meanwhile, the top five SMPs in the UK were: Facebook (54.89%), Twitter (20.17%), Pinterest (13.97%), Instagram (6.15%), and YouTube (1.81%)¹⁴ (Statcounter, 2024b). Although the same five platforms were listed in both countries, their rankings were different. To understand the most used platforms in both, I calculated their average percentages in both India and the UK in 2019, with the results of:

1. Facebook with 71.69% average.
2. Twitter with 11% average.
3. Pinterest with 8.78% average.
4. Instagram with 4.35% average
5. YouTube with 2.5% average.

These demographics provide insights into the context of social media in both countries and help explain why I chose to focus on Facebook and Twitter platforms in my research (see Section 5.3).

In summary, while the numbers addressed at the state level reflect the population dynamics constructing both countries, the demographics provided on the digital sphere - the internet and SMPs - illustrate their digital populations. Understanding these demographics is important, as the intersection of offline and online populations highlights the interplay between traditional and digital governance.

3.2 Political System

Given a political system's role in shaping digital governance through policies and regulations (see Chapter 2), this section examines it within the democracies of

¹³ Followed by LinkedIn (0.09%), Reddit (0.07%), and Other (0.11%) (Statcounter, 2024a).

¹⁴ Followed by Tumblr (1.62%), Reddit (0.83%), and Other (0.55%) (Statcounter, 2024b).

India and the UK. To achieve this, this section is divided into three subsections: form of government, party politics, and elections.

3.2.1 Form of Government

India and the UK have different forms of democratic governance. To explain this, I provide a brief background on the creation and functioning of their democratic governments and discuss their separation of powers - first on India and then on the UK.

Although democracy is relatively new in India, it is referred to as the largest democracy in the world due to its population (O'Neil, 2023). Upon gaining independence from British colonial rule in 1947, India formed a federal parliamentary political system. The government is separated into three branches under the Constitution. It consists of the executive as the President (serving ceremonial head of state) and the Prime Minister (head of government) (Soni, n.d.). It has a bicameral legislature consisting of Rajya Sabha (Council of States) and Lok Sabha (House of People) (Soni, n.d.). Finally, there is the independent judiciary, headed by the Supreme Court of India (Soni, n.d.). At the time of my research both the President, Droupadi Murmu, and the Prime Minister, Narendra Modi, were from the Bharatiya Janata Party (BJP).

The UK is one of the world's oldest democracies and transformed from a monarchy into a democratic state in 1832 under the Reform Act. It operates as a constitutional monarchy and a parliamentary democracy. Devolution granted Scotland, Wales, and Northern Ireland separate legislative and executive bodies that focus on local governance (Devolution: Factsheet, n.d.). The central government of the UK has three branches: the executive, legislature, and judiciary. However, this apparent separation of powers is actually 'fused', since the Prime Minister needs majority support from the House of Commons to govern (Chris Brown, 2019, p. 4). This was seen in 2022, when the Conservative Party had to change Prime Minister thrice in two months (Gregory, 2022). Such power dynamics help maintain democratic practices among branches of government, reinforcing the UK's political system as a strong democracy.

Understanding these state governance systems is crucial, as it illustrates the allocation of power among government units which help to understand how digital policies are formulated, implemented, and enforced. This context sheds a light on comprehending the governance systems that have constructed the two countries' digital governance (see Chapters 6 to 8 for findings).

3.2.2 Party Politics

To understand the ideology behind the political context of each countries' governance, this subsection provides context on the ruling and the main opposition parties in India and the UK.

India's contemporary politics is dominated by the ruling Bharatiya Janata Party (BJP), with the Indian National Congress (INC) as the main opposition¹⁵. Unlike coalition governments formed between 1989 and 2009 elections, the 2014 election marked single-party dominance under the BJP in India (Jha and Choubey, 2023). The BJP's rule was viewed as transforming the political atmosphere of the country from a secular state to a hegemonically Hindu state (Jha and Choubey, 2023). It was argued that it advocates for 'Hindutva (Hinduness)', which rejects multicultural values and aims to define India through Hindu values (Al Jazeera, 2019). This religious-ideological foundation of the BJP-led government has generated debates about the character of Indian democracy, leading to discussion about it being a hybrid regime¹⁶, where 'key democratic institutions have remained formally in place', but 'norms and practices underpinning democracy have substantially deteriorated' (Tudor, 2023, p. 121). In contrast, the INC (also known as the Congress party) has declined since the rise of the BJP (Jha and Choubey, 2023). Unlike the BJP, the Congress does not bind itself with pro-Hindu values, and tends to be more inclusive (Arun, 2013). However, one of the prevailing critiques against the INC is that it had gained power for 'personal enrichment' of those involved, rather than long-term nationwide growth (Arun, 2013).

¹⁵ Other parties include the Communist Party of India, the Aam Aadmi Party, and the National People's Party.

¹⁶ See Chapter 2 for 'hybrid regime' definitions in the literature.

At the time of my research, the UK's political party context was dominated by the ruling Conservative Party and Labour Party as the main opposition¹⁷. The Conservative Party was formed in 1834 and is the oldest political party in the UK. They had been in power since 2010 and won the 2019 general election, forming a government with Boris Johnson as Prime Minister¹⁸, although he was later replaced by Liz Truss and then Rishi Sunak¹⁹. The party is associated with centre-right ideologies that support free-market principles and strong national defence. In contrast, the Labour Party was established in 1900 in response to the Conservatives and Liberals (Garnett *et al.*, 2021). Unlike the Conservatives' free-market ideology, the Labour Party is rooted in the labour movement and located more on the centre left, seeking social justice and workers' rights (Garnett *et al.*, 2021).

Although both countries were ruled by single-party dominant governments between 2019 and 2023, they had clear differences. To compare them, I refer to the Freedom in the World reports²⁰. Reports show that India has not achieved a full freedom score on political pluralism and participation²¹, while the UK was awarded a full score²². This reveals a freedom difference between party politics in India and the UK, complementing the context provided in this subsection. Taken together, this provides insights into existing political parties in both countries and their freedoms, which informs about the political context that may shape policies and frameworks in relation to their digital governance.

3.2.3 Elections

As representative democracies, both India and the UK hold elections, where citizens vote for members to represent them in parliament. Appreciating this state-level context is crucial for understanding digital governance, since elections increasingly intersect with the digital sphere, where online campaigns, misinformation and manipulation can directly impact on the electoral processes of democracies (see Chapters 1 and 2). To provide context on elections, this

¹⁷ Other political parties include the Liberal Democrats, and the Green Party of England and Wales.

¹⁸ Until 2022.

¹⁹ Remained as the PM during research period in 2023.

²⁰ See Appendix 1, B, India.

²¹ See Appendix 1, B, India.

²² See Appendix 1, B, United Kingdom.

section focuses on both countries' electoral processes and highlights debates about the 2019 elections in India and the UK.

India's electoral process is controlled and regulated by the Election Commission of India, under the Constitution. The Commission reported a turnout of more than 67% of the population at India's 2019 general election (Jain, 2019). What I found interesting from the secondary sources was that, although India met democratically free and fair election standards²³ in the Freedom in the World reports, Freedom on the Net reports documented instances where social media content was being restricted and allegedly manipulated through bots and inorganic activities by groups associated with political parties²⁴ during elections. One illustrative example cited in Freedom on the Net concerns allegations that the BJP paid private companies to artificially boost its social media content during the 2014 elections (Kritika, 2017, and Biswas, 2017, as cited in India-FoN, 2019).

The UK holds two main elections - general parliamentary elections (Westminster) and regional elections to form parliaments in Scotland, Wales, and Northern Ireland. The body responsible for general elections is the Ministry of Justice, which also coordinates elections for devolved assemblies (Garnett *et al.*, 2021). In the 2019 general election, the turnout was 67.3% (Uberoi, 2023b, p. 5). According to Freedom in the World, the 2019 election was deemed to be free and fair²⁵. However, as in India, Freedom on the Net reported concerns about content manipulation during election period in the UK, including fake news, doctored images, and bots²⁶. One prominent incident reflecting these broader concerns was the Cambridge Analytica scandal, which involved allegations that the firm used Facebook data to deploy data-driven techniques to influence voters during the 2016 referendum on whether to remain in the European Union (EU) or exit it ('Britain-exit', 'Brexit') (Parliament.UK, 2018, as cited in UK-FoN, 2021).

²³ See Appendix 1, A, 2020-2022, India.

²⁴ See Appendix 2, A, B, C, 2019-2021, India.

²⁵ See Appendix 1, A, 2020-2022, United Kingdom.

²⁶ See Appendix 2, B, 2019-2021, United Kingdom.

In summary, both countries had general elections in 2019 with similar voter turnout, where the incumbent governments remained in power. Both have specific institutions to oversee the electoral process. However, information obtained from the Freedom House reports exposed a difference of freedom scores during the 2019 elections in terms of state-level (Freedom in the World) and the internet (Freedom on the Net), revealing a risk of content manipulation online. This underscores not only the importance of digital governance but also complements the previous two chapters on manipulated content during elections in the context of India and the UK.

3.3 Social Diversity

This section addresses diversity and pluralism within the social contexts of India and the UK. To achieve this, it is divided into three subsections: gender (in)equality in political participation, understanding minority groups, and the effectiveness of civil society organisations.

3.3.1 Gender (In)equality in Political Participation

Understanding gender (in)equality provides insights into the political participation of women and people who are identified as LGBTQ+, and their involvement in state governance, which can further help to comprehend their engagement and participation online.

Indian traditions stem from patriarchal roots in which the social context is dominantly centred on men, while women are seen as ‘second class citizens’, and transgender people are ‘perceived as third-class or non-citizens’ (Sahu, 2023, p. 1). Nonetheless, there have been positive changes to address gender imbalance in India. For instance, women started participating in local politics following a constitutional amendment in 1993, and the Supreme Court changed homosexuality from a criminal offence under colonial law²⁷ into a legal right in 2018 (Sahu, 2023, pp. 55, 68). However, gender inequality has not been eradicated in the country. For instance, although the highest number of women MPs were elected to the Indian parliament in 2019, this was only 14.6%,

²⁷ ‘Chapter 16, Section 377 of the IPC, 1860’, (Sahu, 2023, pp.55, 68).

consisting of 78 seats (Verniers and Ammassari, 2019). Considering that women made up almost half of the Indian population in 2019, 634 million people (Global Data, n.d.), this demonstrates a very low involvement in politics. In fact, Freedom in the World reported that gender played a role in political participation²⁸ and personal freedoms²⁹.

In contrast, feminism and the LGBTQ+ movement have gained traction and social acceptance in the UK. Freedom in the World accorded a complete score on the inclusion of gender in political participation³⁰ and practice of personal freedoms³¹ in the UK. There have been debates about women increasingly taking up government roles since the late 1990s (Garnett *et al.*, 2021). To be more specific, the highest number of female MPs ever elected in UK history was in the 2019 election, with 220 female MPs in the House of Commons (Evans, 2020). However, considering that there were 1.3 million more women than men in 2019, 33.9 million (Clark, 2024), there is still need for more female participation in the House of Commons.

In sum, although both countries had the highest number of female MPs voted into their parliaments in the 2019 elections, there was a clear number of differences between India (78), and the UK (220)'s female MPs. Understanding this state-level context on participation was important, as it may inform possible societal outcomes of participation in their digital spheres.

3.3.2 Understanding Minority Groups

Another aspect to consider social diversity is through minority groups in India and the UK. This not only helps to understand their democratic contexts but also sheds a light on the voices that might be transmitted to places in the digital, especially SMPs. Considering different social settings in India and the UK, I specifically looked into religious minorities in India and ethnic minorities in the UK, based on the available data.

²⁸ See Appendix 1, B-4, India.

²⁹ See Appendix 1, G-3, India.

³⁰ See Appendix 1, B-4, United Kingdom.

³¹ See Appendix 1, G-3, United Kingdom.

Although India was formally deemed a secular country under the Constitution (Forty-Second Amendment) Act (1976), religion plays an important role in Indian politics. India is the world's most Hindu-populated country - 79.8% Hindus, followed by 14.2% Muslims and 2.3% Christians (Kramer, 2021). According to Freedom in the World, Indian society is dominated by Hindu practices and beliefs, which affect the civil liberties and individual rights of those in 'minority' groups³². This indicates religious obstacles and division in Indian society but also expands on the role of religion observed regarding the BJP (see Subsection 3.2.2).

Considering its long history of invasion and migration, the UK has migrants from Europe, previously colonised lands, Commonwealth nations, and people seeking asylum from countries where they are in danger (Peace and Meer, 2020). This has not only increased the country's religious and cultural diversity (Peace and Meer, 2020), but also their political representation in the UK. Studies show that minorities have participated in Parliament since 1987 (Peace and Meer, 2020), and 66 MPs from minority ethnic groups were elected in the 2019 election - a majority in the Labour Party (Uberoi, 2023a). Moreover, Freedom House reports indicate the UK's efforts to minimise migration-related issues³³.

Overall, unlike India, my research found the UK to be more inclusive of its ethnic minorities at the state level, illustrating potentially more equitable access and representation for them in online spaces. Considering the use of SMPs as a liberating technology, and the shaping of government regulations to control these in the literature (see Diamond, 2010, in Chapter 1), both countries' attitudes towards minority groups inform their potential approaches to digital governance, policies around content, digital participation, and platforms' accountability to address these issues.

3.3.3 The Effectiveness of Civil Society Organisations

As discussed in Chapter 2, civil society organisations are considered as one of the multi-stakeholders in the digital sphere (Flyverbom *et al.*, 2019). They play an important role in protecting individual rights and enabling social participation in

³² See Appendix 1, D and G, India; Appendix 2, B, India.

³³ See Appendix 1, D and G, United Kingdom; Appendix 2; B, United Kingdom.

a democracy (Boje, 2021), which encompasses issues related to the digital sphere as well. To provide background on this, I provide some context on civil society in both countries.

India's civil society consists of non-governmental organisations (NGOs), advocacy groups, and grassroots movements, which all contribute to Indian democracy. They each act as a check on governmental power and play a vital role in promoting social justice in the country. For instance, they have played a key role in the consultation on and formation of legislation, including the Right to Education Act (2009) and the Right to Information Act (2005), which advanced transparency and accountability measures in India (Hakeem and Sulphey, 2023; Jha and Choubey, 2023, p. 2). However, despite the fact that civil society is effective in raising certain issues, the government 'tries to control the civic sector' (Hakeem and Sulphey, 2023, p. 6) through license permits, restricting funding, imposing surveillance, and limiting fundamental rights for what it deems state security reasons. This not only demonstrates the challenges civil societies experience in India but also highlights the use of technology against them by the government. Likewise, both Freedom House reports note that civil societies have been affected in both the offline and online spheres³⁴, showing that, even though these civil society organisations are trying to help strengthen Indian democracy, the government uses several methods to undermine them.

Civil society in the UK encompasses a diverse range of groups and organisations that operate independently of the government. These include 'clubs, pressure groups, political parties, and religious organizations' (Garnett *et al.*, 2021, p. 605), which provide ways for individuals to participate in public debate and make an impact on society. For instance, pressure groups can get involved in consultations on legislation making at different levels (Garnett *et al.*, 2021). One of the campaigns by a LGBT rights group, Stonewall, was seen to play a role in advocating for the development of the Marriage (Same Sex Couples) Act in 2013 (Milmo, 2010; Stonewall, n.d.). Moreover, while Freedom in the World gave the UK a full score in relation to associational and organisational rights, the country did not achieve full freedom on the FoN³⁵. This divergence might be an

³⁴ See Appendix 1, E, India; Appendix 2, B and C, India.

³⁵ See Appendix 1, E, United Kingdom; Appendix 2, B and C, United Kingdom.

indicator of differing conditions for civil society organisations at the state and digital levels in the UK.

In summary, the discussion above highlights key differences between the two countries, where Indian civil society groups experienced some backlash from the government while those in the UK had experienced a more democratic and inclusive environment at state level but holds freedom concerns in the digital sphere. Such a difference highlights the extent of their ability to operate freely and effectively at state level, which provides essential information about their capacity to advocate for equitable digital governance.

3.4 A Brief Historical Context: 2019-2023

This section provides some context on trending issues and prevailing aspects of the two countries at the time of my research. Considering the timeliness of the topic, these recent changes provide essential information that might impact on digital governance. This section is divided into two subsections: key changes and incidents, and Freedom in the World versus Freedom on the Net.

3.4.1 Key Changes and Incidents

To understand the environment in which my research took place, key moments and aspects of this period are discussed here. This includes a detailed overview of the 2019 general elections, the COVID-19 pandemic, protests, and recent legislation.

First, both countries held a general election in 2019. In addition to the political aspects discussed in Subsection 3.2.3, this similarity provided an important channel through which to explore India and the UK's digital governance, especially through their technological operations and legal management, and the consequences that this might create for the public or state in general. This required careful examination, as political interference can shape discourse, for instance by platforms targeting advertisements and misusing data (see my discussion of Cambridge Analytica in Subsection 2.1.1). Moreover, keeping in mind the literature's emphasis on hybrid and authoritarian regimes to hold elections, like democracies (see Chapter 2), understanding the free and fair

environment of the digital sphere is important in comprehending India and the UK's democracies online.

Second, both governments had to deal with the global COVID-19 pandemic, starting in late 2019. The pandemic was a public emergency, and both governments imposed national and state lockdowns to contain it. Thus, it affected state governance due to the need to protect the public but also challenged the two democracies' digital governance in several ways, as people relied mostly on information and communication technologies to arrange their permitted social interactions.

Third, major political protests happened between 2019 and 2021 in both countries. In India, there were two protests against the BJP government. While those protests for the Citizenship Amendment Act (2019) challenged religious discrimination brought in via an amendment made in 2019, where the government refused to provide citizenship to Muslims, the farmers' protest was against new policies that disadvantaged small farmers in India (S., 2021). In contrast, the UK had Black Lives Matter protests, after a police officer in the US killed American George Floyd (Mohdin *et al.*, 2020). This shows that the protests that happened in India and the UK were linked to their political systems and social diversity contexts detailed above, like the ruling government's Hindu values and corruption in India, and ethnic diversity in the UK.

Finally, both democracies were working to expand their legislation on digital governance during this period. These comprise India's new law, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021), which focuses on controlling digital content and regulating intermediaries. This legislation requires intermediaries to comply in order to be allowed to continue operating in India, which indicates potential influence on its digital governance of SMPs. The UK passed its Online Safety Act (2023), focusing on promoting a safe digital sphere and controlling harmful content, which, like India, provides a possible influence on its digital governance of SMPs.

3.4.2 Freedom in the World versus Freedom on the Net

This subsection provides an overview of Freedom House's freedom scores on the two countries during my research period. Freedom House is a non-partisan organisation that has been measuring countries' freedom levels since 1973 (Freedom House, n.d.). It publishes annual reports containing numerical scores and rankings, which evaluate if a country is free, partly free, or not free, and provides a narrative report for each measuring question (Freedom House, n.d.). The reports I referred to most in writing this chapter were their Freedom in the World (FiW) reports, which focus on state-level freedom in countries.

Additionally, I briefly mention their Freedom on the Net (FoN) reports, which focus on online freedom. Although my research used the FoN narrative reports as a method of data collection (see Chapter 5), it is worth reminding that this is a pre-research chapter, thus, the points made here were not part of my analysis but are simply given here to provide context using the freedom scores awarded to India and the UK.

The Freedom House reports showed that India's freedom score on FiW had dropped from 'free' to 'partly free' in 2021³⁶ for reasons including religious discrimination in politics and against groups including minorities and civil societies (India-FiW, 2021). Meanwhile, India's FoN remained 'partly free' between 2019 and 2021, which demonstrated not only that there were issues around freedom on the digital level, but also its long 'partly free' state when compared to the FiW. In contrast, the UK scored 'free' in both the FiW³⁷ and FoN reports³⁸ between 2019-2021. Despite this, it is important to note that the FoN reports³⁹ gave the UK a lower evaluation score than FiW⁴⁰. What emerged from these freedom scores was that both India and the UK scored lower in terms of their online freedom (FoN) than they did at the state level (FiW). This observation raised the question of why their freedom scores were lower digitally, highlighting the importance of conducting my research into

³⁶ Appendix 1.

³⁷ Appendix 1.

³⁸ Appendix 2.

³⁹ (With an average of 77.6%.)

⁴⁰ (With an average of 93.3%.)

understanding and investigating the issues encountered with their digital governance.

3.5 Conclusion

This chapter has provided background information on India and the UK, covering their state and digital demographics, political systems, social diversity, and historical contexts. Each of these aspects contributed to understanding the interplay between traditional and digital governance, offering a foundation for my research findings (Chapters 6 to 8). While the demographics revealed the populations in both offline and online spheres, the political systems highlighted the governance frameworks and explained how power was distributed. Social diversity reflected on inclusivity and representation within their societies, whereas the historical context underscored recent changes in both countries. Together, these four sections enabled me to ascertain a holistic view of the environment in which their digital governance operated, providing a comprehensive basis for their examination.

The next two chapters describe my analytical framework and the methodological design of how I conducted my research into the digital governance of India and the UK.

Chapter 4 Analytical Framework

This chapter describes the analytical framework I used to explore digital governance in India and the United Kingdom (UK). It draws on the complexities of digital governance highlighted in the literature review (see Chapter 2) and the two countries' different characteristics and socio-political contexts as outlined in Chapter 3. This chapter is divided into two sections: liberal internationalism and a structuration model of digital governance. Liberal internationalism comprises a normative foundation for evaluating the Indian and UK democracies' governances in the digital sphere. However, it does not cover the operational dynamics of digital governance, which is why I have developed a more nuanced theoretical lens, the structuration model of digital governance.

4.1 Liberal Internationalism

Liberal internationalism is a school of thought studied in both political and international relations, which combines principles of liberalism and internationalism. I first discuss liberalism, its adaptation in international relations and institutions, and then I describe the role of the United Nations (UN) and its workings in relation to democracies, digital governance, and human rights.

Liberal principles advocate for democracy, the rule of law, a free market economy, and human rights (Collins *et al.*, 2022). Although rooted in the Enlightenment period and the workings of Immanuel Kant, Jeremy Bentham, and John Stuart Mill, liberalism has evolved significantly to address modern global challenges, especially after the two World Wars (WWs) (Dunne, 2023). Liberal internationalism builds on these liberal principles and applies them to the anarchic international system, where no overarching authority exists. It posits that states are rational actors, and their cooperation could prevent war, foster developments, and act collaboratively during difficult times (Collins *et al.*, 2022; Dunne, 2023). To achieve these goals, liberal internationalism emphasises the global rule of law, universal rights, and the role of international institutions (Owen, 2018; Collins *et al.*, 2022) to mediate relations between individual countries, to 'safeguard the security and liberty of each' (Owen, 2018, p. 102).

One of the most momentous achievements of liberal internationalism post-WWII was establishing the United Nations (UN) in 1945. The UN has become the world's largest intergovernmental organisation, with 193 member states (United Nations, n.d.). Unlike regional organisations that have specific socio-political and cultural interpretations, like the European Union, the UN demonstrates a more universalist approach and an international standpoint, providing a normative objectivity for my comparative case countries which are from different regions.

The UN and its leading bodies, like the General Assembly and Human Rights Council, continue attempting to enhance democracy globally, with the aim of maintaining peace, developing 'friendly' relations between states, helping them fight poverty, and encouraging them to protect universal rights and freedoms (United Nations Information Service, n.d.). One of its most significant achievements is the Universal Declaration of Human Rights (UDHR), which was published in 1948 and lists the rights that every individual should be entitled to, regardless of race, gender, religion, or ethnicity (Universal Declaration of Human Rights, 1948). Although these rights are not legally binding, its foundations and principles have influenced state regulations. Even though these rights were created in a post-war environment before the invention of ICTs, the UDHR covers some rights that exist in the digital age, like the right to privacy and freedom of speech. This is shown by Resolution A/HRC/RES/42/15 of the Human Rights Council, which affirms that the offline right to privacy stated in the UDHR covers the digital sphere as well (the Office for the United Nations High Commissioner for Human Rights, 2019). This not only demonstrates the UN's adaptation to technological developments, but also indicates the universalist aim to protect rights in the digital sphere.

In summary, by adopting liberal internationalism as the normative foundation of digital governance, my research investigated both India and the UK's protection and preservation of individual rights online and the rule of law to assess their digital governance structures.

4.2 Structuration Model of Digital Governance

This section describes the theoretical framework I developed to explore the digital governance of SMPs in India and the UK, which I call a **structuration model of digital governance** (also referred to as digital structuration). This framework provides a comprehensive analysis model through which I examined the complexities of digital governance practices exhibited broadly by governments, SMPs, other stakeholders, and citizens in India and the UK. To explain how I devised this original framework, this section is divided into four subsections. The first subsection introduces Giddens' structuration theory, its constituting features, and other scholars' critiques of his theory. The second subsection expands on this by integrating a technology element into it, using Orlikowski's duality of technology. The third subsection addresses the interpretative approach Walsham adopted in his analytical framework for organisational change and information systems, emphasising the subjective and socio-political dimensions of understanding technology. The fourth subsection synthesises all of these frameworks and describes my own innovative theoretical framework of the structuration model of digital governance.

4.2.1 Structuration Theory: Anthony Giddens

Building on his works from the 1970s, Giddens developed the theory of structuration in his book 'The Constitution of Society' (1984). Although this was before the invention of the World Wide Web and discussions about digital governance, his theory provides a valuable framework for my research. To explain its relevance, I discuss the core features of structuration theory, outline three components that I used to build my theoretical framework, and highlight its critiques with my responses.

Structuration theory provides a holistic lens through which to study interconnected relationships of structure and agency. Giddens (1984, p. 2) described structuration theory as 'neither the experience of the individual actor, nor the existence of any form of societal totality, but social practices ordered across space and time'. By structure, Giddens (1984) meant rules and resources (allocative and authoritative), and he used 'agency' to refer to individual or collective actors with the capacity to act in a society. However, acknowledging

the intentional and unintentional actions of an agent, Giddens distinguished 'agency' from agent, where agency referred to the capacity of power to act and make decisions in a society intentionally (1984, pp. 5-16). Put differently, an agent is the actor performing actions, and agency is the potential and power inherent in those actions. These dynamic interactions between structure and agency produce social systems, which result in 'any ongoing, patterned social relation' (Appelrouth and Edles, 2007, p. 529) - systems that evolve across time and space. Given its flexibility and openness to adopt change, this overall proposition can be applied to understand digital governance as a distinct social system.

Structuration theory contains three key features that informed building my framework. First, duality. Giddens (1984, p. 25) asserted that structure provides rules and resources affecting human action, while agency reproduces the structure through their actions. He argued that these are not independent, but constitute each other, illustrating a form of 'duality'. From a digital governance perspective, this duality can be observed in how governments or digital platforms shape user behaviour through their structure (such as policies or algorithms), while users' actions simultaneously influence and reshape the structure over time (like public interest or consumer behaviour).

The second feature is agents' own reflexive monitoring. Giddens (1984, p. 5) asserted that individuals continuously assess their own behaviour and surroundings, which results in re-shaping their actions. In the context of digital governance, reflexivity reveals how agents - whether individuals/users, states, or digital companies - reconsider their actions in response to what they have been exposed to online.

The third feature is the concept of power. Giddens viewed power as being embedded between agency and structure. According to this, the agent's power relies on its ability to 'act otherwise' (Giddens, 1984, p. 14). The structure has properties that promote forms of 'domination and power', which are composed of not only materials and allocative resources, but also organisational and authoritative resources like 'infrastructural' ones (Giddens, 1984, pp. 18, 258). I applied Giddens' conception of the power within structure to explain the multi-

stakeholder nature of the digital sphere (see Chapter 2), while recognising that the power of agency refers to users' ability to make their own judgements, which then reshapes the digital space through their interactions and choices.

Structuration theory provides a holistic framework through which to understand dynamics of change over time and space. However, I also took the criticisms which have been levelled against it into consideration when devising my theoretical framework. For instance, Archer (1982) criticised the idea of mutually constituted structure and agency in a social system, arguing that this implies a unified system where the two cannot be separated. Instead, Archer (1982) proposed a morphogenesis in which structure and agency can be separated and evolve over time. However, Giddens' point about the reproduction of social systems posited that structure and agency are not rigidly bound but dynamically interact, shaping each other. Thus, dynamic interplay captures the co-construction and complexities of social systems, like digital governance, and Archer's notion of morphogenesis. In other words, rather than separating the units to study the social system at different spaces and times, structuration theory proposes a way to understand the formulation of those systems which can transform as a result of such interaction.

Another challenge to Giddens' theory came from Bhaskar (1979), a critical realist, who argued that structure exists independently from agency, and shapes and influences the way agency operates. However, this critique does not account for reciprocal relationships in all social systems. For example, in the context of democratic governance, the structure-agency duality is evident, where citizens vote in elections to form governments, and governments control states where citizens participate. Although the government (structure) influences society, society (agency) retains the power to vote and reshape the government. This illustrates that structure is not entirely independent of agency within the context of governance, supporting Giddens' argument and application of his theory in my research.

Despite being criticised by other scholars, structuration theory provides a unique framework for studying continuous changes and transformations in society. Its

flexible and adaptive design has been expanded by other scholars, such as Orlikowski, which helped me design my theoretical model.

4.2.2 The Duality of Technology: Jane Orlikowski

Orlikowski (1992) drew on Giddens' structuration theory to examine the interaction between technology, humans, and organisations. Expanding on Giddens, Orlikowski (1992, p. 405) integrated technology as a third dimension alongside structure and agency. From an agency perspective, she stated that 'technology is created and changed by human action, yet it is also used by humans to accomplish some action' (Orlikowski, 1992, p. 405). This underscores technology's duality relationship with agency, as it is both a product of human agency and a tool that influences human actions. From a structure point of view, Orlikowski argued that, once technology is created and given meaning by humans, its employment becomes 'institutionalized', meaning that technology loses its human element and becomes integrated with the structure, where it maintains a duality with institutions (Orlikowski, 1992, p. 405). On the one hand, institutional decisions influence technology's use on the human level, such as the availability of products, laws, and resources; while on the other, technology shapes and transforms structures at institutional levels (Orlikowski, 1992, p. 410). This exposes the dynamic nature of technology, in that it is part of the changing social system and plays a role in the way it gets shaped and interacts with society.

Following Orlikowski's framework, I integrated technology as the third dimension of my theoretical framework, focusing on the dynamic interplay of technology, agent/agency, and structure. Whilst acknowledging Orlikowski's approach on technology's duality with agency and structure, I call their interplay a triadic dynamic in my framework, where all elements interact to co-create digital governance practices. For example, social media platforms (technology) are regulated by governments' legal frameworks (structure) but also shaped by users' behaviours (agency). By examining their triadic interplay, my framework could be used to identify patterns that developed a comprehensive understanding of a social system, which is digital governance. I applied this to create a comprehensive framework that covered multi-dimensional aspects of digital governance at the macro, meso, and micro levels. While Giddens'

structuration theory illustrated the mutual constitution of macro (structure) and micro (agent/agency) levels of understanding, Orlikowski's approach to technology mediated the interaction between structure and agency/agent, a meso-level consideration. I interpreted the entities she called 'organizations' in her theory as SMPs in my research. To further develop the interpretative and contextual dimensions of my framework, the next subsection explains how I integrated Geoff Walsham into my structuration model of digital governance.

4.2.3 Interpretative Research: Geoff Walsham

I expanded my model by integrating Walsham (1993)'s 'organisational change and IS: synthesised analytical framework', to acknowledge the importance of context and the role of social and political contexts in dynamic environments. Since my research considered the digital governance in the two democracies and focused on SMPs, my research covered fields such as political science, legal studies, sociology and media studies. Thus, integrating Walsham's concept into my framework ensured that the interplay between technology, structure, and agency could be approached and adopted by interdisciplinary fields of digital governance.

While Walsham (1993) drew on several theories like critical theory, hermeneutics, and postmodernism, he also integrated structuration theory as a central component to his framework. He synthesised insights from Giddens' modalities on 'interpretative schemes, facilities, and norms' and Orlikowski's institutional adaptation to structuration theory, to create an analytical framework for understanding change in organisations (Walsham, 1993, pp. 64-66). Walsham's framework consists of four elements: content (structural understanding and changing of the organisation), social context (the relations between participants), social process (cultural and political perspectives driving change), and social context and social process linkage, which means interpreting the effect of structuration on information systems (Walsham, 1993, pp. 68-9). Thus, through understanding structural and individual-level interactions, Walsham's framework sheds a light on the changing dynamics of organisations by focusing on their information systems.

Similar to Orlikowski, Walsham (1993, p. 5) used the word organisation to refer not only to the information systems located in an organisation's departments, but also the 'sectoral, national, and international context within which the organisation is located'. His multi-dimensional perception of organisation provides a useful lens for my structuration model on digital governance. To explain this, I re-interpreted the four elements of his framework as follows: 'content' referring to the governance and technological structure, 'social context' as the SMP environment, 'social process' as countries (India and the UK) adaptation of digital governance and their prevailing socio-political contexts, and the 'social context and social process linkage' as the interpretation of structuration on digital governance. Thus, his framework underlined the interplay between technology (in my research this was the technical features dependent or independent of SMPs), structure (state governance or SMP governance), and agency (public views) from an interdisciplinary standpoint, which helped me to construct my framework.

4.2.4 Creating 'the Structuration Model of Digital Governance' in India and the UK

I synthesised the three theoretical frameworks described above to create an original, comprehensive framework for studying digital governance as a social system, with a specific focus on SMPs. To explain how I achieved this, I first define structure, agency, and technology within the context of my research, depicted in Figure 4.1. Second, I outline three key features of my framework. I conclude this subsection by discussing how I applied this framework in my research on India and the UK.

First, in the context of my research, structure consisted mainly of the rules and resources (allocative and authoritative resources) of key stakeholders including nation-state governments (including their departments, laws, regulations, and systems), and SMPs (such as their platform policies and design). It was important to recognise these two key players in my research, as governments are not the only actors controlling the allocative sources within digital governance, due to its multi-stakeholder nature. By allocative resources, I mean not just 'material features, means of production, and produced goods' (Giddens, 1984, p. 258), but digital governance resources, which includes dual-use technologies, data,

platforms, technical and non-technical operations, and so on (see Chapter 2 for more examples). Thus, such a transformation of allocative resources in different times and spaces diversifies authoritative controls, involving governments and SMPs, as the structure of digital governance systems.

Due to my research's specific focus on India and the UK's contexts, I expanded my definition of structure by incorporating the other theoretical frameworks discussed above. For instance, structure refers to the institutionalisation of technology whose meanings were given by humans, as argued by Orlikowski. This means that institutions determine the law, availability of the product, and resources about a technology (see Section 4.2.2). In my research, this referred specifically to India and the UK's laws and regulations in using and providing technology to agents. I expanded on this by incorporating Walsham's interpretative approach to information structures, asserting that the content - which is the structural understanding of the governance - and the role of institutions shape the context, where political and social practices and processes help people to comprehend the environments where technology is used and humans interact. This not only enabled me to study digital governance in the contexts of India and the UK, but also to investigate their digital governance as two democracies, following my liberal internationalist normative framework (see Section 4.1). Overall, structure had ruling, managerial, and interpretative capacity within my digital governance framework.

Second, I defined agent and agency separately. Within the context of digital governance an agent is an individual or collective of users operating online. Their capacity to act illustrates a connection to the social context posited by Walsham, highlighting the interactions between users in the given Indian and UK societies. In contrast, agency refers to agents who have access to power and make intentional decisions on digital governance. This encompasses not only users who are aware of and make reflexive decisions about their actions, but also agency from different organisational levels, like policy makers, governments, and SMPs. Drawing on Walsham's multi-dimensional view of organisations, this perspective helped me to address the triadic engagement of digital governance - for example, users' capacity to intentionally engage with the content they see on platforms, SMPs' engagement with governments while

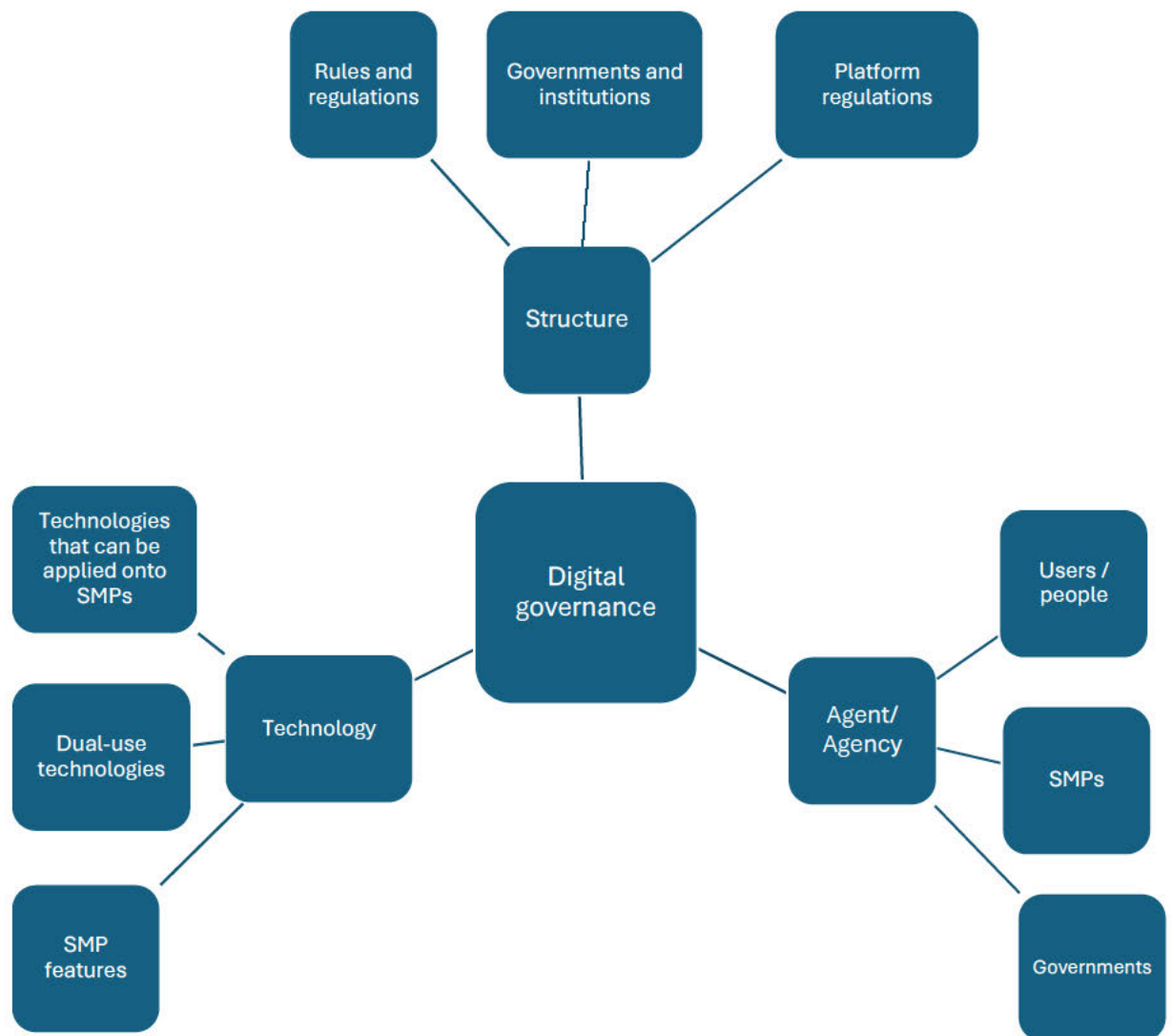
holding the power to decide when to share users' data with those governments, or where the governments adjusted their regulatory frameworks in response to the former two agencies.

I expanded my definition of agent and agency by integrating them with Orlikowski's human element from her duality of technology framework and Walsham's interpretative approach. As discussed in Subsection 4.2.2, Orlikowski argued that humans do not just invent technology, but also give meaning to it, which then becomes institutionalised and part of the structure. This not only underscores technologies' triadic engagement with agency and structure but also highlights Walsham's interpretative approach in how we perceive information systems, which refers to digital governance in this context. Instead of analysing the technological aspect in isolation, Walsham's framework emphasises socio-political understanding and incorporates interpretation into this theory. Considering the multi-dimensional agencies described above, in my study this meant understanding that the governments, SMPs, and users could make their own interpretations of the technology when using, developing, and intentionally engaging with them. For instance, despite both democratic and authoritarian regimes' adoption to the same digital sphere, as outlined in Chapter 2, the literature showed different interpretative uses and developments of technology from these regimes. Considering this within the context of my research, I refer to India and the UK governments' construction of digital governance of SMPs, the technological features, and how this was perceived by people. Acknowledging this interpretative engagement with technology is crucial in understanding agency's duality with technology, but also with governments, since it continues to be in triadic engagements with structure and technology.

Third, I defined technology as any digital item, tool, method, or operation that was created or used as part of India or the UK's digital sphere. Based on my initial literature review and the background context to my case study countries, in this thesis the term 'technology' includes features of SMPs, dual-use technologies (see Chapter 1), and digital governance operations highlighted in my literature review (see Chapter 2). From a theoretical standpoint, this expanded on Giddens' allocative sources; technology within the context of the digital governance of SMPs can be perceived as a diversification of allocative

sources in a different time and space, the cybersphere. Thus, technology became a distinctive element of my structuration model of digital governance, influencing institutions in terms of their operations and regulatory mechanisms as well as becoming a tool and product of individuals (like Orlikowski's duality framework).

Figure 4.1: Structuration model of digital governance of social media platforms



Drawing on the above description, I defined the structuration model of digital governance as the framework of a social system which is comprised of the intertwined triadic relations of the structure, agent/agency, and technology, to argue that they mutually constitute, transform, and (re)create the digital governance of SMPs. To explain this definition further, I integrated the three

features of Giddens' structuration theory outlined in Subsection 4.2.1 into my framework.

The first feature is that these three aspects have a mutually constitutive relationship, which is triadic, building on Giddens' duality of structure and Orlikowski's duality of technology. Within the context of my research, this meant recognising that each aspect of technology, structure, and agency were all in intertwined engagements with each other, resulting in a constantly changing digital governance. While these relationships remain mutually constitutive, my framework allowed for analytical reflection on the relative causal primacy of each aspect within specific empirical contexts.

The second feature I incorporated into my theoretical framework was the reflexive monitoring of the agency, as discussed in Giddens' structuration theory (Subsection 4.2.1) - where the agent and agency change their actions depending on their environment. Given the description I provided in my framework outline above, this means that not just users, but also SMPs and governments, are actors who make intentional changes.

The third feature I integrated into my framework was Giddens' interdependent definition of power, where power is divided between the structure, agent/agency, and technology in my model. For instance, in my research the power of structure encompassed authoritative sources such as regulatory and managerial issues (like laws), agent/agency as the power to make changes (like narratives or voting in elections), and technology (available tools or media channels).

In summary, the framework I developed entailed analysing the interplay between governments, laws, users, social and political contexts, platforms, and other digital technologies within the contexts of India and the UK (some of which were explained in Chapter 3). These preliminary features informed the development of my theoretical framework and provided a comprehensive approach to analysing the dynamic and constantly changing nature of digital

governance. I reflect on this framework further in Chapter 9, following the discussion of my empirical findings on India and the UK⁴¹.

4.3 Conclusion

This chapter has presented the analytical framework used in my research, which consisted of a normative foundation and a theoretical framework. Adopting a liberal internationalist stand justified my research approach in comparing two democratic countries from different regions. This normative foundation foreground not only my empirical focus on integrating the workings of the UN and the UDHR principles, but also my goal to explore how India and the UK have adopted them within their digital governance. Furthermore, I have described how I developed an innovative theoretical framework - my structuration model of digital governance - in order to inform the approach followed in my research. It drew on three theoretical frameworks centred on structuration, combined with technology and interpretative approaches. This original framework not only contributes to interdisciplinary studies on the digital sphere but also provided an alternative way to study the complex dynamics of digital governance. Overall, this analytical framework aided my research design and data analysis, which will be discussed in the next chapter.

⁴¹ Giddens' theory of structuration is suitable for empirical studies, while Orlikowski and Walsham's work has demonstrated its application to case studies, which aligned with the design of my research (see Chapter 5).

Chapter 5 Research Design and Methodology

This research adopted a comparative case study design to examine the digital governance of SMPs in India and the UK. It followed an inductive approach and reflexive methodology to explore complexities within the two countries' contexts. To explain how this research was conducted, this chapter is divided into seven sections. Section 5.1 explains the philosophical underpinnings of my interdisciplinary research. Section 5.2 explains my research questions in detail. Section 5.3 presents my comparative case study design, followed by Section 5.4, which details my multimethod approach. Section 5.5 describes the three stages of my multimethod approach, consisting of secondary data analysis (Subsection 5.5.1), online interviewing (Subsection 5.5.2), and synthesis and validation (Subsection 5.5.3). Section 5.6 lists the ethical considerations. Section 5.7 concludes the chapter by addressing the limitations of my methodological framework.

5.1 Philosophical Underpinnings of my Interdisciplinary Research

Scholars define interdisciplinary studies as those which address complex questions that require more than one discipline (Repko *et al.*, 2014; Szostak, 2015). To explain the approach followed in my research, I first discuss my social constructivist ontology and then my critical-constructivist epistemology.

My ontological position opposes the idea that there is only one way to study the world, arguing that there are multiple realities, as things transform in an interconnected way (Berger and Luckmann, 1966, p. 34). Berger and Luckmann (1966, p. 70) argue that 'social order exists only as a product of human activity'. A constructivist-based ontology underpins my theoretical framework, used to address understanding the agent, technology, and structure of the dynamic levels of digital governance. It highlights that society is under continuous development and engagement. This can be traced through to Giddens' duality of the structure and reflexive monitoring of the agent, where both mutually constitute each other in modern states. It also addresses the way technologies are integrated within societies, following the concept of the social construction of technology (SCOT). SCOT posits that technology is not independent of society

but is socially constructed (Hughes, 2012) by societal groups that raise problems and shape technology (Bijker and Pinch, 2012). In addition to the social construction of human actions and technology, my research addressed the importance of institutions, since they are also socially constructed and play a role in shaping technology (Klein and Kleinman, 2002). Through this social constructivist approach to society, technology, and institutions, my research has established a world view that perceives the continuous social construction of reality, including the interplay of actors on digital governance.

My research took a critical constructivist stance to studying digital governance in India and the UK. This combines the critical school, social constructivism, and Science and Technology Studies (STS) (including SCOT). The critical school is rooted in understanding the dominant power that controls a society (Hesse-Biber *et al.*, 2015). Despite focusing on power and controls, these scholars agree with some aspects of social constructivism within the scope of critical constructivist epistemology. For instance, they align with Bijker's use of empirical methods and opposition to notions of technological determinism like SCOT, while emphasising the role of politics, economics, and interventions from democracies in social construction (Feenberg, 2017). Acknowledging also the role of technology in societies, this mixed stance leads to a critical constructivism which is 'concerned with the threat to human agency posed by the technosystem' (Feenberg, 2017, p. 38). Feenberg (2017, p. 159) defines a technosystem as 'a field of technical practices aimed at control of the environment, whether natural, economic, or administrative'. My research interpreted a 'technosystem' as part of the social system of digital governance my theoretical framework focused on (see Section 4.2). Using this critical constructivist epistemology enabled me to uncover power dynamics, technological practices, and societal responses, to understand the triadic interplay of technology, structure, and agent/agency in digital governance. Together, these philosophical foundations provided a cohesive approach for studying the complex interplay in digital governance.

5.2 Research Questions

To investigate how India and the UK digitally govern SMPs, I conducted an empirical study to examine the triadic relations of digital dual-use technology, legal framework, and the public. To achieve this, I devised two main research questions: **‘How do India and the UK construct their digital governance in relation to social media platforms?’** and **‘What is the broader significance of this for democracies and digital governance?’** To address these questions, I generated three sets of sub-research questions (SRQs):

- SRQ.1 What are the existing digital dual-use operations involving social media platforms in India and the UK? Who conducts these operations?
- SRQ.2 How do legal frameworks inform the regulation of digital dual-use operations and stakeholders? What legal concerns are raised regarding the digital governance of social media platforms?
- SRQ.3 What implications and concerns do experts raise regarding the digital governance of social media platforms and their impact on the public in India and the UK?

SRQ.1 examined existing digital dual-use⁴² operations that involved SMPs in India and the UK. This provided a contextual understanding of which dual-use technologies were employed and by whom, highlighting the multi-stakeholder nature of digital governance in both countries.

SRQ.2 explored the legal landscape regarding social media governance in India and the UK. It focused on the regulations of digital dual-use operations and platforms, as well as the protection of individual rights. This analysis was further supplemented by the concerns raised by my respondents. Following my liberal internationalist foundation (see Chapter 4), this question integrated the Universal Declaration of Human Rights (UDHR) and assessed its adaptations and protections within the domestic frameworks of both countries.

SRQ.3 examined experts’ concerns and observations regarding the impact of digital dual-use operations (SRQ.1) and the legal environment (SRQ.2) in India and the UK. By incorporating insights from experts and relevant secondary data,

⁴² See Subsection 1.2.2 for a detailed discussion of dual-use technologies.

this question sought to uncover the observed public influence and their responses to digital governance in each country.

These empirical findings informed my analysis of the main research questions, contributing to an understanding of how digital governance is constructed and continuously shaped in relation to social media platforms in India and the UK. The answers obtained led to further discussions in relation to the significance of these for democracies and digital governance.

5.3 Research Design: Comparative Case Study

My research adopted a comparative case study design, focusing on two countries and two social media platforms (SMPs). Simons (2009, p. 21) defines case study research as ‘an in-depth exploration from multiple perspectives of the complexity and uniqueness of a particular project, policy, institution, program or system in a “real life” context’. Considering that digital governance operates at the intersection of the digital sphere and real-world contexts, like legal and socio-political systems, my research encompassed both the digital and the state aspects of digital governance.

The design I used aligned with George and Bennett’s (2004, p. 76) concept of a ‘building block’ case study, which focuses on examining ‘particular types or sub-types of a phenomenon to identify common patterns or serve a particular kind of heuristic purpose’. By comparing and contrasting India and the UK, I was able to identify common patterns between their digital governance of SMPs, such as the governments’ relationship with the platforms, legal frameworks, and my respondents’ perceptions of the digital governance implications and concerns for the public. These patterns informed theory generation (George and Bennett, 2004), contributing to broader digital governance insights.

Using case studies in qualitatively driven research does not require pre-determined variables and promotes flexibility since it follows an inductive approach, allowing in-depth exploration (Simons, 2009). However, to guide my multimethod approach (see Sections 5.4 and 5.5), I incorporated three pre-defined variables rooted in the research questions for guidance. The first two, digital dual-use and legal frameworks, were treated as independent variables,

while respondents' perceptions were considered dependent variables in understanding how my case countries construct their digital governance. These variables remained flexible, allowing new variables or definitions to emerge during analysis, ensuring that the final themes or patterns determined from comparing and contrasting my case studies were robust.

Case selection was a critical component of my comparative case study design. George and Bennett (2004, p. 83) emphasise that case selections are an 'integral part of a good strategy to achieve well-defined objectives of the study'. The primary units of my analysis (De Vaus, 2001, p. 220) were two case countries, while the two secondary units were SMPs embedded in these countries. To ensure valid comparison and contrasting through my case countries, I used the sampling criteria outlined below.

The first criterion was countries that had democracy as their system of state governance. This criterion emerged from the research gap I identified in the literature, where democracies had practiced some digital authoritarian and non-democratic practices.

The second criterion was countries that had adequate technological development integrated into the state at a degree that enabled social media management. This was essential for the validity of my research, since comparing and contrasting countries that were dissimilar or had inadequate levels of development could undermine my analysis.

The third criterion was to select countries that had English as an official language. This allowed me to access and use data from primary sources, including official government documents, and a vast number of secondary sources, as well as conducting interviews in English. This enabled language consistency in data interpretation and analysis, while preventing risks of errors in translation.

Using these criteria, I selected India and the United Kingdom as my case study countries. The two SMPs comprising my secondary units of analysis were selected using the following criteria.

The first criterion was SMPs that were used in both India and the UK. This was to ensure valid comparisons of the same platforms in different contexts.

The second criterion was SMPs that were popular. This was to ensure I could find interview respondents who had had adequate workings and expertise in these platforms, and could identify valid operations and legal frameworks, since picking small, unpopular platforms would have undermined my own exploration.

The third criterion was SMPs with Transparency Centres and available secondary data for 2019 to 2021 (see Section 5.5.1 for Stage 1). This was to make sure both platforms had workings in relations to my case study countries.

Following these criteria, I selected Facebook and Twitter. Both platforms were among the most popular SMPs in India and the UK (see Section 3.1). During my research, Facebook changed its name to Meta in 2021, while Twitter's name was changed to X in July 2023. To maintain consistency with the data I collected in this stage, I use their former names in this thesis.

Overall, my comparative case study design narrowed down the focus onto two countries and two SMPs in order to address my research questions (see Section 5.2). By comparing these cases, the study aimed to discover how socio-political and technological factors shape and construct the digital governance of SMPs. This serves as a building block study that contributes to interdisciplinary studies on digital governance internationally.

5.4 Qualitatively Driven Multimethod Approach

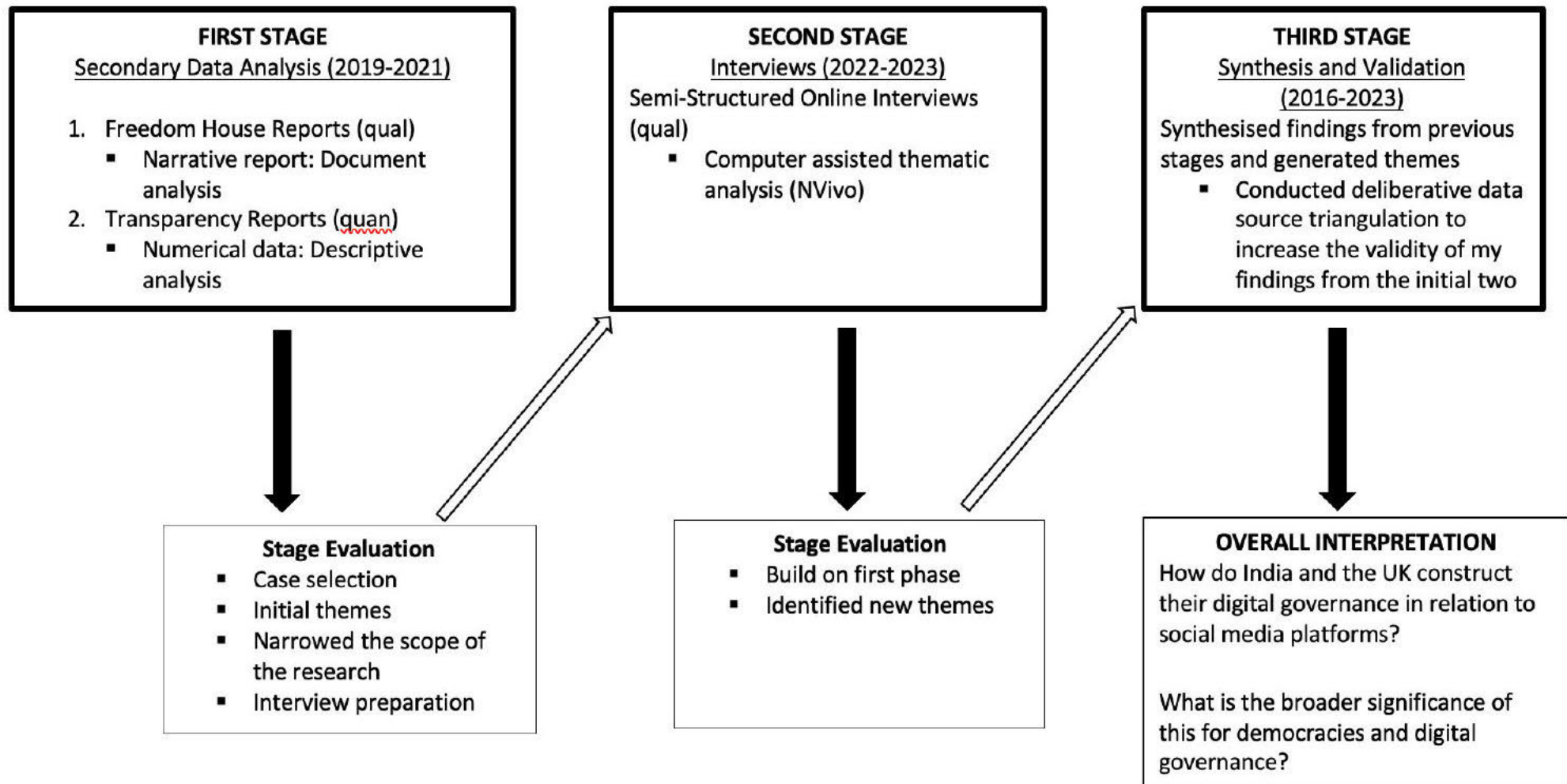
My research adopted a qualitatively driven multimethod approach within its comparative case study design. The multimethod approach entails collecting data from multiple sources to obtain an in-depth understanding of the research context and find answers to research questions (Sandelowski, 2000; Mason, 2006). Given the flexibility this approach provides when combining qualitative and quantitative methods (Hunter and Brewer, 2015), I prioritised qualitative data over quantitative data, which acted as auxiliary information.

To compare and contrast India and the UK through the two platforms, I designed a multimethod study with three sequential stages of data collection (see Figure 5.1):

- The first stage obtained data from secondary data, comprising Freedom on the Net narrative reports (qualitative) and transparency reports from Facebook and Twitter (quantitative), from 2019 to 2021. I employed document analysis to evaluate the narrative reports and descriptive analysis to examine the transparency reports, generating my initial research themes.
- The second stage involved conducting 22 semi-structured online interviews with respondents who had expertise in different aspects of digital governance in India and the UK. These were conducted in 2022 to 2023 and then analysed using NVivo, to identify key themes.
- The third stage entailed synthesising the findings from my secondary data analysis and interviews, further evaluating the validity of my results derived from these initial stages. To ensure the credibility and rigour of my findings, deliberative data source triangulation was conducted, corroborating findings with relevant existing secondary data. This iterative process refined the analysis, enhanced consistency, and strengthened the validity of my research findings. This stage focused on data sources covering the period from 2016 to the end of 2023.

Throughout these three research stages, I dealt with the data reflexively. The first two stages included a 'stage evaluation' phase, where I reflected on the data collection, interpretation, and initial themes, and was able to make adaptive responses to the methodological needs of my research. This was to ensure alignment between my research questions and data collection with my case studies and to strengthen the comparative analytical robustness of my findings. This reflexivity not only prepared each stage for the following one but also ensured that the choices were well informed and capable of addressing the complexities of digital governance in India and the UK.

Figure 5.1: Multimethod comparative case study design



5.5 Methods

5.5.1 Stage 1: Secondary Data Analysis

The first stage of my research comprised secondary data analysis, which Hakim (2000, p. 24) defines as ‘any reanalysis of data collected by another researcher or organisation’. I analysed two types of secondary data in this stage, qualitative and quantitative. For qualitative, I used the narrative reports from Freedom on the Net (FoN). For quantitative, I used the two SMPs’ transparency reports. Given my qualitatively driven multimethod approach, the FoN reports held greater analytical weight and provided a deeper understanding, while the quantitative data from the transparency reports served as supporting data. To ensure consistency and validity of my mixed secondary data analysis in this stage, I limited these datasets to those covering the years 2019 to 2021. This limitation enabled a timely multi-year comparison of India and the UK across different sources. The rest of this subsection explains why I selected these reports, outlines their relevance to my research, describes how the data were collected and analysed, and concludes with some reflexive remarks on this first stage.

I made an informed decision to integrate FoN reports into my analysis following my contextual research of using Freedom House reports in Chapter 3. The annual FoN narrative reports cover 12-month periods from June to May, so the reports I used covered June 2018 to May 2021⁴³. The reports measure countries’ internet and digital media freedom by asking 20 questions in three categories: ‘obstacles to access, limits on content, and violations of user rights’ (Freedom on the Net - About Freedom on the Net, n.d.). I analysed FoN reports using document analysis, through which I decided which questions to focus on.

Document analysis is an iterative process. Bowen (2009, p. 34) defines it as ‘evaluating documents in such a way that empirical knowledge is produced, and understanding is developed’. This method allowed me to observe changes over time and refine my research scope prior to the second stage (Bowen, 2009, pp.

⁴³ See Section 5.7 for more discussion on ‘Limitations’.

29-30). As it is the responsibility of a researcher to provide information, present steps, and techniques (Bowen, 2009, p. 29), I describe the four steps I followed when analysing the narrative reports below.

The first step was preparing the documents for analysis, which I did in two ways. I started by creating tables for each FoN question on India and the UK, from reports from 2019 to 2021 (see Appendix 2). Then, I reviewed questions that fell under the scope of my research questions, according to the guidance of my pre-defined independent (digital dual-use and legal frameworks) and dependent⁴⁴ (concerns and implications about digital governance on the public) variables.

The second step entailed conducting a systematic reading of the potentially relevant questions and initial coding to start building themes. In the light of my guiding variables and research questions, I focused on identifying recurring issues related to the digital governance of social media platforms in the two country contexts. Following this systematic reading, I selected 16 out of available 21 questions as the basis for my initial coding. The five questions I left out were outside my research scope, including topics like the infrastructure, cost, and demographics of service providers, as well as non-SMP related details (see Appendix 2 for the full list of FoN questions). The selected questions covered topics involving the use of dual-use technology, operations, public incidents, legislation, individual rights, and democracy-related events. I coded them manually, using pen and highlighters, to identify recurring issues, concepts, and emergent themes that were pertinent to my research. The 16 questions I coded are set out below.

- The ‘obstacle to access’ category provided insights into the technical management and controlling of digital infrastructure in the Indian and UK contexts, which encompassed understanding the service providers. It included the following questions:
 - A.3: Does the government exercise technical or legal control over internet infrastructure for the purpose of restricting connectivity?

⁴⁴ Given their expertise and long-term study internationally, including on India and the UK, I incorporated FoN findings within the scope of ‘experts’ in my research (see SRQ.3).

- A.5: Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?
- The ‘limits on content’ category provided a comprehensive assessment of digital content in India and the UK, relating to my variables of digital dual-use operations, legal frameworks, and the prevailing impacts and concerns on the public. This included the following questions:
 - B.1: Does the state block or filter, or compel service providers to block or filter, internet content?
 - B.2: Do state or non-state actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete the content?
 - B.3: Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?
 - B.4: Do online journalists, commentators, and ordinary users practice self-censorship?
 - B.5: Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?
 - B.7: Does the online information landscape lack diversity?
 - B.8: Do conditions impede users’ ability to mobilize, form communities, and campaign, particularly on political and social issues?
- The ‘violations of user rights’ category provided a comprehensive overview of the legal frameworks in India and the UK. This including their national legislation, individual rights, and regulations of the digital sphere, making references to specific operations like surveillance and encryption. I used seven questions listed in this category:
 - C.1: Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?
 - C.2: Are there laws that assign criminal penalties or civil liability for online activities?

- C.3: Are individuals penalized for online activities?
- C.4: Does the government place restrictions on anonymous communication or encryption?
- C.5: Does the state surveillance of internet activities infringe on users' right to privacy?
- C.6: Are service providers and other technology companies required to aid the government in monitoring the communications of their users?
- C.7: Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?

The third step focused on turning the codes identified in Step 2 into themes. To achieve this, I divided a wall-mounted pinboard into two, half for each country, and started pinning my codes up based on their connections (see Appendix 3 for pictures). These groupings demonstrated some prevailing differences in terms of the operations, associated laws and impacts of those. This inspired me to theme my codes along the digital dual-use operations conducted by different socio-political actors or companies, which narrowed the scope of related legal frameworks and public outcomes. As a result of this process, I generated three themes from FoN which each had three constituent aspects.

The last step involved writing initial thematic comparisons and contrasting points of India and the UK and undertaking some reflexive decisions on how to present my FoN document analysis. Although I generated initial themes based on my FoN data coding, I presented these identified issues and aspects as a review within my document analysis framework to describe the contextual underpinnings of each country in the finding chapters (Chapters 6 to 8). While writing this review, I observed the benefit of integrating secondary original source references listed in these reports for a detailed presentation of my findings. Thus, I integrated my informed snowball literature review with the sources cited by FoN, such as laws, news articles, research reports, and journals. To provide further detail on the law I analysed, I created an appendix containing legal extracts and notes (see Appendix 4). Together, this approach supported

the validity of my FoN findings and enhanced my comparative analysis by enriching the context on India and the UK.

The other secondary data I used was from Facebook and Twitter's Transparency Centres, which both provided several longitudinal reports. To select reports to use in my research, I used the following criteria.

The first criterion was reports that both platforms had on India and the UK. As described in Section 5.4, although India and the UK were my primary units of analysis, the two social media platforms were embedded in my research as secondary units. That is why, for my research validity, the reports I collected from Facebook and Twitter had to be closely linked.

Second, the selected reports needed to cover the 2019 to 2021 period to align with the time frame defined for this stage. Accordingly, I focused on reports regarding government user data requests⁴⁵ and content removal⁴⁶. Both platforms published their reports on a six-monthly basis. To interpret the data within the context of my research, I followed three steps in my descriptive analysis to review these reports.

The first step of my descriptive analysis involved extracting quantitative data from the transparency reports and preparing this for analysis. I started by compiling data into tables and then categorised them by platform, type of report, and country; this resulted in eight tables (see Appendices 5 to 12). Each of these eight tables provided six numerical values bi-annually over three years, 2019 to 2021, for both countries.

The second step was deciding which data units were comparable, due to some observed differences in the ways Facebook and Twitter published their reports. Facebook's 'Government Requests for User Data' reports documented data on total requests, legal process requests, emergency disclosure requests,

⁴⁵ Called 'Government Requests for User Data' by Facebook, and 'Information Requests' by Twitter.

⁴⁶ Called 'Content Restriction Based on Local Law' by Facebook, and 'Removal Requests' by Twitter.

users/accounts requested, and % of data produced (the % of government requests fulfilled by Facebook) (India-Facebook, n.d.-b; UK-Facebook, n.d.-b). In contrast, Twitter's 'Information Requests' reports presented emergency, routine and combined numbers for each information request, their compliance rate and accounts specified, and separately detailed the preservation of accounts and requests (India-Twitter-Web Archive, 2022; UK-Twitter-Web Archive, 2022)⁴⁷. To ensure data comparability, I focused on the total number of user data requests, number of accounts requested, and platforms' compliance rate with the requests made by Indian and UK governments to both platforms.

The content removal tables also revealed some differences between the two platforms. Facebook's 'Content Restriction Based on Local Law' reports provided data on the amount of content restricted (this encompassed data on the selected country, restrictions applied to other countries, and global restrictions) and restrictions by products (such as album, comment, page and group, post, profile, and event) (India-Facebook, n.d.-a; UK-Facebook, n.d.-a). In contrast, Twitter's 'Removal Requests' reports included legal demands, compliance rate, accounts specified, accounts and tweets withheld, and account Terms of Service (TOS) (which referred to accounts removed for breaching platform policies) (India-Twitter-Web Archive, 2022; UK-Twitter-Web Archive, 2022). Facebook's content removal in line with the countries' local laws differed from Twitter's processing of government requests, like its information requests discussed above. To contextualise these in my case countries, I analysed both platforms separately. I used Facebook's total number of content pieces restricted and the restrictions by product in India and the UK. Meanwhile on Twitter, I focused on the number of legal demands received to restrict accounts and the numbers of withheld content in India and the UK.

The third step was to identify if there was any change over time. I did this by measuring the four reports' 'raw score changes' data in the two countries, quantitatively calculating the change in scores every six months from 2019 to 2021 (De Vaus, 2001, p. 156). This quantitative analysis employed descriptive

⁴⁷ See Section 5.7 for 'Limitations' and why I used Web Archive.

statistics; I counted average numbers in the reports to determine typical values and did a range analysis to identify the highest and lowest reported figures in the reports published within three years. My representation of this analysis used either numerical or percentage figures and, when possible, was supported visually with graphs and tables in Chapters 6 to 8. This analysis provided auxiliary data to governments' engagement with the SMPs, i.e. supporting evidence to ascertain the affected numbers of users and content in this regard.

Taken together, the secondary data was used for my foundational analysis of existing information in relation to digital governance in India and the UK. This stage not only shaped my understanding of the digital governance landscape in India and the UK but also prompted two significant reflexive considerations for my research.

First, I integrated my analysis of SMP reports with the themes I had generated from FoN reports at the end of this stage. This provided supplementary data to two of my themes and identified the need for further assessment in the interview stage to either address or re-define the third theme at the end of the synthesis.

Second, the data analysed in this stage helped me narrow my scope of my research in both countries in terms of identifying key operations, laws, issues and incidents related to the digital sphere. These themes informed Stage 2 by guiding my respondent selection and interview question design, covering topics like technological operations, legislation, and key civil organisations. Overall, this reflexive engagement with the data, which was central to my multimethod approach, ensured alignment across my stages and increased the validity of my research.

5.5.2 Stage 2: Semi-structured Online Interviews

The second stage entailed collecting primary research data with the objective of getting insights from individuals who had expertise and experience related to the dynamic aspects of digital governance in India and the UK. This directly contributed to SRQ.3 while complementing Stage 1 and contributing to

answering the other SRQs. To ensure I obtained rich insights, I developed a sampling strategy that targeted individuals who had experience in one or more aspects of digital governance. Below, I outline this strategy, explain the online interview method, and detail my analytical approach used in this stage, which combined thematic analysis with selective discourse analysis.

Considering the interdisciplinarity of digital governance, my sample units could have ranged from areas including information technology, digital law and policy, journalism, human rights, activism, and academia, as inspired primarily from the literature review (Chapter 2), context provided on the two states (Chapter 3), and insights observed in Stage 1. Although I was flexible about which sectors to draw my samples from due to the complexity of digital governance, I imposed certain criteria, which can be explained in three points: sample criteria, sample size, sample sourcing, and recruitment.

First, I purposefully defined my sampling strategy and included respondents who had expertise or experience of working on various digital governance aspects in India and the UK. This ranged from people in NGOs or think tanks to journalists, activists, civic activists or organisations, researchers, and technology professionals, as detailed further below. It was vital that they had expertise in the political, social, historical, or broader digital context of India or the UK (see Chapter 3). To ensure I collected relevant primary data, I excluded respondents who were not resided or from India or the UK. This ensured that my respondents had lived experience within the respective country they were interviewed on.

As a result, I conducted 22 interviews with people from different sectors in India and the UK, 11 per country. In line with my ethical considerations (see Section 5.6), all respondents have assigned pseudonyms to protect their anonymity. These names are used consistently to contextualise their perspectives and aid clarity in presenting my findings. Table 5.1 lists my 11 Indian respondents, which comprised a lawyer and policy counsel working on digital technologies (Deepa), a policy counsel on digital rights (Ravi), a lawyer on the internet freedoms (Priya), a journalist working on technology (Sanjay), an investigative journalist working on issues related to the digital sphere (Amit), a security analyst on democracy

and technology (Nikhil), a public policy professional on law and technology (Tarun), a policy director working on the impact of technology and digital rights (Vikram), a lawyer on personal data (Manish), an academic lawyer on the impact of technology and democracy (Karan), and a research associate in privacy and data governance (Arjun).

Table 5.1: Participants from India		
Respondent Number	Occupation/Job Title	Pseudonym
Indian Respondent 1	Lawyer and Policy Counsel	Deepa (female)
Indian Respondent 2	Policy Counsel	Ravi (male)
Indian Respondent 3	Lawyer	Priya (female)
Indian Respondent 4	Journalist	Sanjay (male)
Indian Respondent 5	Investigative Journalist	Amit (male)
Indian Respondent 6	Security Analyst	Nikhil (male)
Indian Respondent 7	Public Policy Professional	Tarun (male)
Indian Respondent 8	Policy Director	Vikram (male)
Indian Respondent 9	Lawyer	Manish (male)
Indian Respondent 10	Academic Lawyer	Karan (male)
Indian Respondent 11	Research Associate	Arjun (male)

As shown in Table 5.2, my 11 UK respondents were a legal and policy officer working on data protection and privacy (Tom), a solicitor and campaigner on individual rights (David), an author working on digital authoritarianism and technology (Richard), a legal officer on digital human rights (Claire), a consultant on free information (Sarah), a researcher on the use of data in politics (Emily), a retiree from the IT sector who is also an author on dual-use technology products and personal data (Mark), a journalist on information security (Anna), an academic journalist on data politics (Jessica), an academic consultant on the use of data (Rachel), and a researcher on the role of digital media (Lauren).

Table 5.2: Participants from the UK		
Respondent Number	Occupation/ Job Title	Pseudonym
UK Respondent 1	Legal and Policy Officer	Tom (male)
UK Respondent 2	Solicitor and Campaigner	David (male)
UK Respondent 3	Author	Richard (male)
UK Respondent 4	Legal Officer	Claire (female)
UK Respondent 5	Consultant	Sarah (female)
UK Respondent 6	Researcher	Emily (female)
UK Respondent 7	Retiree from IT Sector and Author	Mark (male)
UK Respondent 8	Journalist	Anna (female)
UK Respondent 9	Academic Journalist	Jessica (female)

UK Respondent 10	Academic Consultant	Rachel (female)
UK Respondent 11	Researcher	Lauren (female)

Second, my initial plan was to undertake 30 interviews (15 per country) in six months. However, I prioritised data saturation over this fixed number. As Mason (2010) argues, one common mistake made by PhD students is to gather more than enough data for their research. I observed that nodes on NVivo were settled and remained mostly the same after coding five or six interviews in each country, while the child nodes that emerged showed alignments in respondents' points at the end of 18-22 interviews. This represented my data saturation point, after which no new nodes were emerging from my interviews.

Third, in terms of sample sourcing and recruitment, I searched for interview respondents on various online channels including Twitter, LinkedIn, websites, and through snowball sampling from my interview respondents. This gave me the opportunity to purposefully select and reach people that held relevant experience and expertise to my research topics.

Fourth, I recruited my respondents by contacting them through emails, Twitter messages, and website forms. On first contact, I described myself and my research and invited them to voluntarily take part in my research. In cases where I made this first contact through emails, I attached my Participant Information Sheet and Privacy Notice to provide further information (see Appendices 13 and 14). This was not possible in Twitter or website forms due to their format, but instead I offered to send an email with these two documents attached to people who were interested. I sent those keen to take part the Consent Form via email and scheduled an online interview (see Appendix 15). With an expectation of low turnout due to the COVID-19 pandemic at the time, I contacted 111 individuals and organisations in India and 106 individuals and organisations in the UK. My interviews with 22 respondents were conducted between April 2022 and March 2023, as described next.

I adopted a one-to-one synchronous online interview method, where a researcher and respondent conduct an interview in real time (O'Connor and Madge, 2017). I used Teams and Zoom software, offering respondents the flexibility to choose which platform they felt comfortable with. As mentioned in Stage 1, I generated some initial questions from the FoN reports, which were open-ended to ensure flexibility for my respondents to answer the questions from their own stances (Braun and Clarke, 2013, pp. 78-79; Fielding and Thomas, 2015, p. 282), whilst ensuring that the interviews remained within the scope of my research (Robson and McCartan, 2016, p. 290). I conducted four pilot interviews - with three colleagues from the University of Glasgow's law school and one friend who is a technology journalist - to test these questions, get a sense of the timing, and consider some sample answers before undertaking my interviews (Fielding and Thomas, 2015, p. 283). These pilot interviews raised the need to generate some personalised questions depending on each respondent's profile, job, and background. This was primarily to allow for people from different sectors to discuss the same topic.

I designed my interviews to have five main sets of questions and to last around 45 minutes to an hour. With the experience obtained from my pilot interviews, these questions were intended to 'introduce, "warm up", main body of interview, and "cool-off" followed by a closure' (Robson and McCartan, 2016, p. 290). I introduced the topic with some general questions on the role of social media in each respondent's life and society:

- 1) I would like to start by asking your views about social media:
 - a) How would you describe its presence in your life?
 - b) How important do you think it is to democracies? And why?
 - c) How would you describe its role and power in [India/the UK]?

I followed up by asking for their views on the ways governments regulate the digital sphere and their opinions on the relationship between governments and social media platforms, which served as the warm-up:

- 2) Keeping in mind the diversity of social media platforms:
 - a) What democratic principles (such as rights and values) do you think are important when regulating social media platforms?

- b) What are your views on the way social media platforms are regulated in [India/the UK]?
- i) (Possible follow-up question if the definition given in the first clashes with the second question)

Then, I moved to the main body of questions regarding dual-use technologies and their implications, as well as gathering their concerns in relation to this. To make sure that my respondents were familiar with the term 'dual-use' and how it is used on social media platforms, I pasted a UK government's definition of dual-use into the chat box during the interviews, alongside some examples from the secondary data analysis as a prompt:

- 3) As part of the research, I would like to ask if you have heard of dual-use technologies?

'Dual-use items include software and technology that can be used for civilian and military purposes' (Export Control Joint Unit, 2021). These are additional and external tools. Common examples identified: content control, censorship, targeting information, accessing data, and surveillance & monitoring.

I then asked the main body of questions and some personalised questions depending on each respondent's profile and background. These included:

- 4) Have you noticed any dual-use tools or operations used on social media platforms in [India/the UK]? If so, what are they (this can be different from the prompts given above and specific to the background of the respondent)?
- a) Would you agree with the employment of these tools on social media platforms?
- i) What would be your concern?
- b) How democratic do you think is the application of these dual technologies on social media platforms?
- i) What democratic principles do you think they would hinder/infringe (linking back to question 2.a above)?
- c) Have you heard any of these or other similar tools practiced on platforms in [India/the UK]? If yes, give examples.
- i) Follow-up question depending on the example
- d) Keeping in mind that those technologies are also used for military and security purposes, do you think the rule of law is enough to control their employment?
- e) How/in what ways do you think they influence individuals (or the public) on social media platforms (like their online activities, self-censorship, individual rights and freedoms)?

- i) Does it affect the trust relationship between the public-and government? How?

Additional questions (personalised)

These questions varied, depending on a respondent's profile, job, and background. For example:

- I asked journalists about their experiences on social media platforms, concerns and observations.
- I asked legal and policy officers specific questions based on their expertise, like data protection, free speech, or platform regulation.

These personalised questions complemented different sectoral workings on digital governance by gathering my respondents' experience and expertise in the two countries' contexts. Following these in-depth discussions, I moved to closure by asking:

- 5) Thank you very much for sparing some time for this interview.
 - a) Is there anything else you would like to add to what we have discussed today?
 - b) Do you have any suggestions of people who might be interested in taking part in this research?
 - c) Would you like to receive a summary of research outcomes at the end of this project?
 - d) Is there anything else you would like to ask before we close?

To avoid any potential technical challenges, I prepared a checklist to work through prior to my interviews. This helped me to follow the interview process consistently, meeting the agreed ethical standards in terms of dealing with and storing personal data (see Section 5.6).

I examined the interview data through thematic analysis. Clarke and Braun (2017, p. 297) define thematic analysis as 'a method for identifying, analysing, and interpreting patterns of meaning ("themes") within qualitative data'. To conduct my thematic analysis, I grouped my respondents' concerns and opinions about the social media platforms, regulatory and legal aspects in the countries, operations and dual-use tools we had discussed, and their observations of how these elements influence the public, among other points that emerged from the transcripts. I followed a structured approach to ensure I thoroughly explored the

interview content (Robson and McCartan, 2016, p. 464) and used the NVivo computer program as a tool which helped me organise my data to generate codes systematically from each interview transcript. My analysis consisted of three steps, as outlined below.

In the first step, I prepared the interview transcripts for analysis. Although my interviews were automatically transcribed on Zoom and Teams, I checked and corrected these drafts to obtain accurate verbatim transcriptions (Fielding and Thomas, 2015, p. 291). This enabled me to familiarise myself with the data and turn documents into a dialogue format to ease my analysis. This was also when I pseudonymised my transcripts by removing all of my respondents' personal information from the research data, keeping the original recordings stored on OneDrive due to ethical considerations (see Section 5.6).

The second step was to upload the pseudonymised transcripts and start coding their data on NVivo. I followed a complete coding approach, rather than selective coding, to maximise the use of my data and explore themes emerging from them. Braun and Clarke (2013, pp. 206-7) describe complete coding as coding 'all the data that's relevant to your research question'. Following the order of my interview questions (see above), I started to group my codes based on the emerging points in each set of four questions, like respondents' views on the social media platforms, democratic principles and regulations in their country, dual-use operations, and concerns and implications they observed in regard to digital governance of SMPs on the public. To achieve this complete coding, I used 'coding stripes' on NVivo, where I sorted my codes into 'nodes' and 'child nodes' (Gray, 2018, pp. 663-4). This approach helped me to identify patterns in the transcripts from both countries. As Seal (2015, p. 445) argues, the coding process is a stage where data can be explored and arranged into categories, instead of solely focusing on its technicality. Considering my thematic approach to analysing the data, coding also served to give meaning to data in the context of my study (Seal, 2015, p. 447). This step resulted in generating six primary nodes and several child nodes, which differed in each node.

In the third step I turned my nodes into themes, using the coding structure reports from NVivo. The six nodes depicted different aspects of digital governance in India and the UK. What partially differed between them was the child nodes, which demonstrated the interpretation of those nodes by the respondents in these countries, while also contextualising them. This was identified through using traditional methods, pens and highlighters, on the coding structuring report. As a result of this process, I produced six themes on India and the UK (see Appendix 16). Some of these themes were similar to the themes from the first stage, such as operations, laws, and individual rights like privacy and freedom of speech, but others were different, as they provided primary insights.

Following the thematic analysis, I integrated discourse analysis as a supplementary method to examine the language my respondents used when expressing their views, positions, and perspectives about digital governance. This reflexive decision was prompted by the recognition that certain respondents had discursive statements that thematic analysis alone could not fully capture. According to Gee (2014, p. 14), discourse analysis is ‘the study of language-in-use’. In my research, ‘language’ refers to the spoken interview data, analysed through textual transcripts. Given the familiarity developed during thematic analysis, I adopted a purposive approach to identify and analyse discursive data. This process unfolded in three steps.

First, I reviewed thematically categorised data to identify quotes in which language reflected discursive features such as binary framing, ideological assumptions, or subject positioning. This served as the initial selection of relevant quotes for discourse analysis.

Second, I conducted a closer reading of selected quotes using Gee (2014, pp. 51-61)’s seven building tasks - significance, activities, identities, relationship, politics, connections, and sign systems and knowledge - as a guide. These seven tasks demonstrated the ways in which quotes carried discursive importance. This helped narrow the quote selection and inform subsequent interpretation.

Third, I deepened the analysis by focusing on who ('socially situated identity') and what ('socially situated practice or activity') of my respondents within interview contexts (Gee, 2014, p. 53). To achieve this, I used Gee (2014, pp. 51-61)'s tools of inquiry: social languages, Discourses (with big 'D'), intertextuality, and conversations. This enabled me to ascertain an understanding of reality from my respondents' lenses within the specific interview contexts, as 'talk is always designed by those who produce it for the context in which it occurs' (Cameron, 2001, p. 145). Acknowledging the importance of context and interpretative reflexivity, given my position as the researcher, I focused not only on the way language was used in that specific context, but also on Discourse, which is 'combining and integrating language, symbols, and objects to enact a particular sort of recognizable identity' (Gee, 2014, p. 51).

In summary, combining thematic and purposive discourse analysis captured both what was said and how it was said, offering a richer, context-sensitive interpretation of my respondents' views. The six themes generated and their purposive discourse analysis provided insights into topics like technology, platforms, democracies, governments, laws, observed implications on the public, and issues within the contexts of India and the UK. Given my reflexive approach, I developed two methodological reflections based on collecting and analysing the semi-structured online interviews, which raised potential implications for how I approached Stage 3.

First, the nature of the data collected in this stage demonstrated personal perspectives and experiences of my respondents from India and the UK. There were instances that I observed possible contextual influences on my respondents at this stage of analysis. For instance, although gender was not a selection criterion, Tables 5.1 and 5.2 indicate differences in gender distribution among my respondents from the two countries. Additionally, I sensed some degree of self-censorship on political issues among my respondents in India compared to those in the UK. While these reflections were not systematically measured, they illustrate some connection to the broader socio-political background given in Chapter 3. This reflection, while potentially a finding on its own, underscored

the need for data source triangulation to enhance the validity and rigour of my findings in Stage 3, following thematic synthesis.

Second, the six themes generated in this stage differed from the three themes developed in Stage 1, providing a more in-depth assessment of digital governance in both countries. This raised the need for a thematic synthesis in Stage 3.

5.5.3 Stage 3: Synthesis and Validation

This stage concluded my research by synthesising findings from Stages 1 and 2 and conducting data source triangulation. The goal of this process was to enhance the validity, robustness, and rigour of my findings.

To begin the synthesis, I created a table containing the three themes that emerged from Stage 1 and six themes from Stage 2. To make best use of my collected data and find answers to my research questions (see Section 5.2), I followed three steps.

The first step specifically focused on the Stage 1 themes and traced their links with Stage 2. While the two digital dual-use themes which consisted of socio-political findings from Stage 1 were also evident in Stage 2, one of these themes only appeared in India and was coded as a child node. Thus, I kept the two themes but also integrated the third theme of Stage 1 as a child node onto one of the main themes.

The second step followed the same approach focusing on Stage 2, where I integrated dual-use operations and their connected aspects identified from interviews onto the two themes listed in the previous stage. However, my interview nodes showed an additional theme which contained digital dual-use and socio-political aspects, making three themes for my research.

The third step was to define the constituting aspects to depict these themes. To achieve this, I re-assigned the relevant sub-themes from Stage 1 and nodes in Stage 2 to the final three themes, which were digital dual-use operations. I used

my constituent codes to define these themes at the start of each finding chapter⁴⁸. This re-distribution generated four aspects of digital governance, covering different technical, legal, and socio-political findings (see Appendix 17).

Since I had followed an iterative process to generate my final themes and acted reflexively throughout this exploratory research, I conducted a data source triangulation to enhance the validity of my thematic findings. Instead of repeating what has already been collected, Stake (1995, p. 109) emphasises the need for a triangulation procedure to show ‘deliberative effort to find the validity of data observed’. While Stake (1995) highlights this as a deliberative method, Denzin (1989) offers a more specific technique for triangulation. He distinguishes ‘data sources’ from ‘methods of generating data’, asserting that data sources are part of triangulation where a researcher just follows the same methods to gather more data (Denzin, 1989, p. 237). Denzin (1989) lists three types of data source triangulation: time, space, and person. I incorporated all three into my research. This enabled a deliberative validation of findings by capturing change over time, incorporating spatial and normative perspectives, and accounting for varied interpretations across actors in the Indian and UK contexts.

For time, I applied a temporal criterion whereby secondary data preceding and following the periods defined in Stages 1 and 2 were selectively integrated only where they directly related to findings identified in the analysis. On this basis, I included FoN reports from 2016 to 2018 to deliberately validate thematic findings associated with earlier periods, such as Brexit and the Cambridge Analytica cases. Additionally, I incorporated secondary data covering the remainder of 2023⁴⁹ as a follow-up validation to findings that emerged from interviews and to account for subsequent developments in relation to my analysis, including the enforcement of relevant Bills into legislation. Together,

⁴⁸ This thesis contains three finding chapters, each addressing a distinct theme defined in the chapter introduction.

⁴⁹ Following the interview stage that was completed in March 2023.

this deliberative data source triangulation expanded the temporal depth of my secondary data analysis and further validated my thematic findings.

For space, I applied a conceptual and normative criterion by incorporating principles from the Universal Declaration of Human Rights (UDHR), as well as relevant domestic legislation, in line with my liberal internationalist framework (see Chapter 4). This allowed domestic operations and regulatory approaches to be assessed against broader normative and legal standards. I not only triangulated these in my findings, with supporting legal extracts and notes provided in Appendix 4 (following the approach described in Subsection 5.5.1).

For person, I applied a sampling and source-selection criterion by incorporating material from different datasets and studies, like public opinion data and research reports, to enrich and cross-validate my secondary and interview data. Given my existing findings from Stages 1 and 2, this process was a targeted and purposeful collection of data sources in accordance with the four aspects. Overall, to maintain consistency of data collection in this stage and ensure contextual relevance, I limited these sources—such as research reports, public opinion data, websites, government documents, laws, news, articles—to those published before the end of 2023.

In summary, my overall interpretation of the research findings explained India and the UK's digital governance of SMPs through three themes and four aspects, which covered digital dual-use operations, legal frameworks, and experts' concerns and observations on the key implications of digital governance for the public.

5.6 Ethical Considerations

Although I outlined my ethical considerations throughout the research process in Section 5.5, here I provide an in-depth explanation of the ethical protocols I followed when conducting interviews. The interviews gathered personal data, some of which was sensitive as it contained political, cultural, and religious content. This affected my ethical application process, data storage and management plans throughout my research, where I followed the University of

Glasgow's guidance. Scholars like Khan and MacEachen (2022, p. 8) argue that online interviews should meet similar ethical standards to face-to-face interviews, so I approached my data collection with careful consideration of the technical challenges, data sensitivity and use in my research. To discuss this in detail, I use Eynon, Fry and Schroeder's (2017, p. 3) three essential ethical concepts for online methods that collect data from human participants: 'confidentiality, anonymity, and informed consent'.

I approached confidentiality and anonymity as interdependent aspects of the interview data. One way I dealt with this was through data storage, which was vital for protecting the confidentiality of the data collected and respondents' anonymity. Since I conducted interviews on two different platforms, Teams and Zoom, I had to follow different storage procedures. While Teams recordings were saved directly to OneDrive, there were two ways to store recordings on Zoom, either on the computer storage or Zoom's cloud storage (Gray *et al.*, 2020). It is worth pointing out that scholars agree that storing data on a secure computer ensures better confidentiality than cloud storage (Buchanan and Zimmer, 2012; Khan and MacEachen, 2022). Similarly, following the university's Ethics Team's advice on computer storage, I encrypted my personal device⁵⁰ before saving Zoom recordings on it. After saving the recordings on my device, I uploaded them onto OneDrive and securely deleted them from my personal laptop. This way, recordings from both platforms remained encrypted on OneDrive, ensuring the protection of their confidentiality and anonymity during data storage.

Another way to explain my ethical consideration of confidentiality and anonymity is by discussing my choice to pseudonymise rather than anonymise sensitive personal data in my research. Anonymisation entails deleting any information that may identify a respondent (Eynon *et al.*, 2017, p. 15), not only a respondent's name, but also their organisation, city, and profession, among other details that may expose their identity. However, considering the continuation of my research that might require access to the original data, I

⁵⁰ Following advice from the University of Glasgow's Ethics and IT teams.

pseudonymised my interview transcripts and created a pseudonym identifier. This allowed me to keep the original recordings on OneDrive, while I worked on transcripts that had been cleared of personally identifiable information. To work with these transcripts efficiently, I formatted the names of my respondents and the transcripts following the pseudonyms listed in Tables 5.1 and 5.2. This ensured the confidentiality and anonymity of my respondents when presenting interview findings. All my respondents' personal information will be deleted after I have completed my doctoral study, while the anonymised data will be retained by the University of Glasgow⁵¹. Thus, my research data management plan supported my ethical considerations for online interviewing.

In addition to these confidentiality and anonymity aspects, informed consent was a core part of my ethical considerations. Informing respondents about the research, their contribution, and rights before an interview is an important responsibility of a researcher (Khan and MacEachen, 2022). As explained in Stage 2 (Subsection 5.5.2), I gave my respondents three documents: the Participant Information Sheet, the Privacy Notice, and the Consent Form (see Appendices 13-15). While the first two documents provided detailed information about the research, their participation, rights, and privacy, the Consent Form required them to select the platform and recording type (audio or video) they preferred and then sign the form as agreement to take part in my research. Since it could have been more challenging to ensure respondents' understanding online than face-to-face (Eynon *et al.*, 2017), I asked my respondents if they had any questions and wanted to go through the documents before starting the interviews.

5.7 Limitations

During my research I encountered four limitations in the data collection and analysis. First, I was limited to online methods of data collection due to the COVID-19 global pandemic which meant I could not travel, since I was comparing countries that are distant from each other. However, I tried to turn this limitation into an advantage by conducting secondary analysis and online

⁵¹ My interview respondents were informed about this, and it was part of the consent form.

interviews, which helped me to connect digitally with people who were in various locations in India and the UK.

Second, I was limited by the reports available from SMPs' Transparency Centres. As detailed above regarding Stage 1, I analysed user data requested by the Indian and UK governments and content removal. Despite the popularity of Facebook's Ads Library, which could have been used to understand the role of advertisements as part of that SMP's operations in my research, I was constrained from doing so for three reasons. First, unlike Facebook, Twitter had stopped publishing advertisements during my data collection period (2019-2021). Thus, using Facebook Ads Library would have created an invalid comparison between the two platforms. Second, the Facebook Ads Library showed different time ranges on 'issues, elections or politics' in India and the UK. While the UK contained data from November 2018, India's data was from February 2019 (Meta Ad Library Report: India, n.d.; Meta Ad Library Report: United Kingdom, n.d.). Third, even though there were records of political parties and authorities on the Facebook Ads Library in both countries from February 2019 on, it was hard to track intermediaries and organisations that might be associated with political parties or actors in both countries⁵². Therefore, the data I collected from the two SMPs were limited to the availability of reports on these platforms and ensuring their comparability.

The third limitation came from Twitter removing information about its transparency reports from its platform in 2022. Although I had already collected and analysed the data for my research by the time this happened, the webpages are no longer accessible. To provide alternative sources for what I have extracted in the appendices for 2019 to 2021, I have cited Web Archive links to my references.

The fourth limitation arose from the periods covered by the FoN reports. As stated in relation to Stage 1 above, the FoN annual reporting span is from June to May every year. This meant that the 2019 report included data from June 2018 to May 2019, while the 2021 report covered June 2020 to May 2021. This

⁵² See Meta Ad Library Reports on India and the UK, given in the bibliography.

resulted in me having to present my findings not as following calendar years from January to December, but in line with the reports published for 2019-2021. In spite of this, the FoN reports still provided valuable and comprehensive information about the digital governance of India and the UK. Considering that this stage entailed conducting secondary analysis, observing such a methodological limitation was expected, as I had re-used the FoN data ‘outside of the original context in which it was collected’ (Moore, 2007).

5.8 Conclusion

Exploring the digital governance of India and the UK through social media platforms was a complex, interdisciplinary, and multi-dimensional project. Building on previous chapters, this chapter has described thoroughly how I conducted my research. By undertaking a comparative case study design and using a multimethod approach, I collected different types of data in order to find answers to my research questions. Through secondary data, online interviews, and data source triangulation (for validation), my study addressed the complexities of digital governance in two national contexts. This methodology’s relevance to my doctoral research lay in its integrative design. By taking a reflexive approach in the way I dealt with the data, I constantly assessed the needs of my research and planned my stages accordingly. As a result, my analysis generated three themes and four aspects which helped me to explain digital governance in the contexts of India and the UK. Appreciating the methodological framework described, this chapter provides essential information for understanding the findings that are presented in Chapters 6 to 8. Moreover, it ensures that the subsequent discussion (Chapter 9) and conclusion (Chapter 10) are firmly grounded on robust methodological foundations.

Chapter 6 -Veillance in India and the UK

-Veillance is the first theme examined in relation to the digital governance of social media platforms (SMPs) in India and the United Kingdom (UK). This chapter presents my thematic findings in four parts.

Part 6.1 provides the socio-political context by addressing government-linked operations and collaborations with external actors regarding -veillance. To achieve this, I categorised -veillance operations identified from FoN reports and supplemented them with interviews and data source triangulation. In doing so, this analysis highlights how -veillance operations were incorporated structurally and explains existing multi-stakeholder engagements in both countries.

Part 6.2 examines -veillance in the context of SMPs. It offers a descriptive analysis of ‘Government Requests for User Data’ recorded by Facebook⁵³ and ‘Government Information Requests’ by Twitter⁵⁴. Then, I incorporated data from my interviews to include respondents’ insights into the role of SMPs. Together, these analyses explain that SMPs are distinct structures with their own systems and act as agents within the scope of -veillance.

Part 6.3 investigates the legal frameworks related to -veillance by analysing individual rights, state legislation⁵⁵, and my respondents’ legal concerns. This required synthesising FoN analysis, interviews, and secondary data for validation. Given my liberal internationalist stance, Article 12 of the Universal Declaration of Human Rights⁵⁶ (UDHR) guided my thematic assessments through the principle of the right to privacy. The goal of this analysis is to explain how both countries’ legal systems interact with technology and agency in the context of -veillance.

Part 6.4 explores my respondents’ insights and concerns they observed about the implications of -veillance on the public. To increase their validity, I synthesised

⁵³ See Appendix 5 for full data on India-Facebook; see Appendix 7 for full data on UK-Facebook.

⁵⁴ See Appendix 6 for full data on India-Twitter; see Appendix 8 for full data on UK-Twitter.

⁵⁵ See Appendix 4 for legal extracts and notes on analysed individual rights and state legislation in both countries.

⁵⁶ See Appendix 4 for legal extracts and notes on the Universal Declaration of Human Rights.

these with FoN and secondary data sources. Each part presents my findings on India and the UK in separate sections. Before presenting the findings, I first define -veillance within the context of my research.

As shown in Table 6.1, my research theme of -veillance consisted of two sub-themes: surveillance and dataveillance. Surveillance encompasses codes that demonstrate ways of monitoring, while dataveillance is the collection, storage, and retention of data collected through various methods listed in the table. Despite their distinct scopes, these thematic operations sometimes overlap, leading to the creation of a broader -veillance theme. As outlined in Chapter 1, I define -veillance as a dual-use operation that can be used for both beneficial and harmful, as well as civilian and military purposes. This data-driven definition, which I derived from my coding process, offers an alternative conceptualisation to existing frameworks, such as Mann's (2013) -veillance plane. Following this contributory definition, I move on to present my research findings on -veillance in India and the UK.

Table 6.1: -Veillance	
Surveillance	monitoring, real-time monitoring, tracking, traceability, encryption/decryption, bulk surveillance, phishing, self-censorship, anonymity, software tools and equipment.
Dataveillance	data collection, data storing, data retention, bulk data collection, retaining data for a certain period, interception, fibre cables, profiling, age verification, information security, and installing recording equipment.

6.1 The Socio-Political Landscape of -Veillance Operations

6.1.1 India

6.1.1.1 Government-Linked -Veillance Operations

Dataveillance Through Regulation

Dataveillance through regulation is a category in which I grouped data collection operations resulting from state policies. Based on the FoN analysis, I identified two ways this is done in India: identity verification and data retention.

The first way emerged from the state's requirement to verify the identities (IDs) of Indian citizens. One example of this is the 'Guidelines for New Mobile Connections', which require service providers to verify customers' IDs before activating their mobile services (Press Information Bureau - Government of India, 2013, as cited in India-FoN, 2020-21). Another example is the Information Technology (Guidelines for Cyber Café) Rules, which require ID verification for those using cybercafés (Department of Information Technology, 2011, as cited in India-FoN, 2016-21). Together, these two examples illustrate how guidelines and regulations result in the collection of data pertaining to Indian citizens' identities.

The second way is through the requirement to retain and store data for a prescribed period of time. One key example I identified on this is the law which requires cybercafés to retain their users' data and share them with the government monthly (Rule 4, Information Technology (Guidelines for Cyber Cafe) Rules, 2011, as cited in India-FoN, 2016-2021). This exemplifies the role of law in data retention and its becoming a form of government dataveillance operation.

The above illustrates that ID verification and data retention are ways in which regulation has resulted in dataveillance in India. This identified method of operation demonstrates a dual effect of regulations. It shows how India's regulatory requirements were shaped by technological contexts, while also illustrating how these regulations influence organisational procedures and result in data collection about individuals. While this subsection has highlighted regulation from an operational focus, the legal discussion regarding data collection is expanded on more in Part 6.3.

Technical Surveillance and Dataveillance Programmes

This category of operation examines -veillance in the form of state-driven infrastructural programmes in India. Using FoN reports, I identified NATGRID, CMS, and NETRA as the three relevant technical programmes. These were also referenced in a petition by the Software Freedom Law Centre (SFLC), a civil society organisation, which argued that the programmes violate the right to

privacy (see SFLC, 2020, as cited in India-FoN, 2021). After outlining each programme, I integrate my respondents' reflections on them illustrate how these systems were constructed in India.

The first programme is the National Intelligence Grid (NATGRID), a database programme that enables 'the investigation and law enforcement agencies' to obtain data from various agencies (Gill, 2020). These 'agencies' include 'Income Tax Departments', 'banks', and 'insurance companies' (Gill, 2020). Since the data stored by these agencies can be used for monitoring and data collection, NATGRID can be used for both surveillance and dataveillance (or simply as -veillance). Moreover, this programme supports my analysis of data retention that results from regulation, as NATGRID relies on data that is already collected and stored by state agencies.

The second programme is the Central Monitoring System (CMS). Unlike NATGRID, the CMS is a surveillance programme that operates through landlines and mobile phones. It allows the government to intercept and monitor citizens' phone activities, including calls, text messages, Voice over Internet Protocol (VOIP) communications⁵⁷, and social media posts (Tiwari, 2017, as cited in India-FoN, 2019-21; Gill, 2020). These interceptions occur via Lawful Intercept and Monitoring (LIM) systems⁵⁸ integrated into service providers (Tiwari, 2017, as cited in India-FoN, 2019-21). FoN reports from 2016 confirm the CMS's operationalisation in New Delhi and Mumbai, illustrating a practical example of how a surveillance programme has been integrated in India (India-FoN, 2016).

The last programme is Network Traffic Analysis (NETRA). Like the CMS, NETRA is a surveillance programme. It uses software developed by the Indian Defence Research and Development Organisation to monitor internet traffic in real time (PTI, 2014, as cited in India-FoN, 2021). However, unlike the CMS's specific focus on phones, NETRA has a more comprehensive scope and monitors internet

⁵⁷ Voice calls made using the internet.

⁵⁸ Under Section 5.1.2 of the Indian Telegraph Act (see Subsection 6.3.1.2).

activity (Gill, 2020). Furthermore, unlike NATGRID, NETRA can access real-time data.

Despite being three different programmes, all these programmes were introduced in 2009. One of my respondents, Arjun, viewed this sudden state-driven development in connection to incidents that had happened in 2008 in India. According to Arjun:

This [referring to surveillance operations] all started after the Mumbai attacks. Like how the US had the 9/11, India had their own 9/11 kind of terrorist attack, which happened in 2008. [...] One of the most precious areas and the most precious hotel was attacked, and a lot of people died there. [...] So that actually brought mindset change in India. [...] This is not about the sitting government or the opposition. [...] We don't have any data on this, but I guess that really triggered the government to move towards this.

This illustrates how a state-level incident might have influenced the development of -veillance operations and their integration into India's digital governance. Arjun's framing of the Mumbai attacks as 'India's 9/11' positions the event as a national trauma that legitimised intensified technical programmes. His echoing of global security narratives, like those in the US following 9/11, indicates how -veillance is seen as an expected state response, regardless of political parties or stances.

Considering the possible accuracy of Arjun's view on the timing of the -veillance operations, the three programmes - NETRA, CMS, and NATGRID - illustrate India's development and integration of large-scale -veillance operations into its governance structure to address security concerns. This category of -veillance operation not only reflects the duality between technology and government but also demonstrates how their interaction influences the security environment experienced by the public, forming a triadic connection between structure, technology, and agency.

Non-Technical Surveillance (Lateral Surveillance)

The final category of -veillance operation that emerged from my analysis is non-technical surveillance, also known as lateral surveillance. This method of

operation can be understood as a de-centralised and interpersonal form of surveillance whereby people monitor their environment. One key example of this is the Cyber Crime Volunteers Programme established by the Indian Cyber Crime Coordination Centre, which is a branch of the Ministry of Home Affairs (India-FoN, 2021). This programme enables ‘good Samaritans to volunteer and register themselves as unlawful content flaggers and help law enforcement agencies identify, report, and remove illegal content’ (The Economic Times, 2021 and Ministry of Home Affairs, as cited in India-FoN, 2021). While this can be seen as a form of deliberative participation in digital governance, it systematically empowers certain individuals with the authority to monitor and report to the police.

One of my respondents, Vikram, criticised the programme’s lack of transparency and the uncertainty it creates in society as it requires ‘citizens to surveil each other, to spy on each other, and then complain or report them to the police’. This criticism depicts a panopticon view of the lateral surveillance programme in India, where peer monitoring is framed as a form of social control. Given this complex yet unique form, the Cyber Crime Volunteers Programme illustrates a lateral surveillance operation that is constituted through the mutual engagement of structure, technology and agency in India.

6.1.1.2 Government Collaboration with Other Actors on -Veillance

This form of operation highlights how external stakeholders and actors collaborated with the government in conducting -veillance operations. My analysis of the FoN reports identified four types of collaboration on -veillance in India. These are purchasing spyware from private companies, government funding of external operations, international collaboration, and data requests made to platforms.

The first operation is purchasing spyware from private companies, notably Pegasus, a dual-use tool sold by Israel’s NSO Group (India-FoN, 2021). Debates over India’s use of Pegasus spyware began in 2019, when WhatsApp accused the government of targeting activists, lawyers, academics, and journalists (Chishti, 2019, as cited in India-FoN, 2020-21). The government’s response can be

ascertained by the Ministry of Home Affairs denying civil society's right to an information request (RTI) on the use of Pegasus (Sharma, 2019, Paliwal, 2019, and BBC News, 2019, as cited in India-FoN, 2021). Despite denying this RTI request, the Ministry of Home Affairs pointed to the law⁵⁹ and stated that 'authorized agencies as per due process of law, and subject to safeguards as provided in the rules can intercept, monitor, or decrypt "any information from any computer resource in the country"' during the parliamentary questioning (Lok Sabha, 2019, as cited in India-FoN, 2020). Although the Ministry neither admitted nor denied using Pegasus, it justified its usability under the law in the Indian parliament.

The second operation entails government funding being used to develop -veillance programmes on SMPs. One such example is the Advanced Application for Social Media Analytics (AASMA), a tool that enables real-time analysis of any data from SMPs. It was developed in 2013-4 by the Indraprastha Institute of Information Technology with funding received from the Ministry of Electronics and Information Technology (MeitY) (Shrivastava, 2018, as cited in India-FoN, 2019). Evidence shows that AASMA has been used by the Indian government, including the central government and 40 departments, since 2018 (Shrivastava, 2018, as cited in India-FoN, 2019). This exemplifies the role of ministerial funding and the integration of an externally developed tool into India's digital governance.

The third is international collaboration against encryption. The Indian government had criticised SMPs for their inadequacy in addressing domestic problems that take place on their platforms (India-FoN, 2021). Together with Japan, India has supported Five Eyes⁶⁰ in making an international statement to Facebook requesting 'law enforcement access to decrypt and provide content in a "readable and usable format"' (Mihindukulasuriya, 2020, as cited in India-FoN, 2021). This international collaboration illustrates not only seven democracies'

⁵⁹ Section 69 of the IT Act and Section 5 of the Telegraph Act (see Subsection 6.3.1.1).

⁶⁰ The Five Eyes countries are the United States, the United Kingdom, Canada, Australia, and New Zealand.

opposition to encryption, but also their critique of anti-privacy measures, and interest in decrypting user information on SMPs.

Finally, the Indian government has requested specific user data from SMPs, including Facebook and Twitter. For instance, the Indian police requested information from platforms including Facebook and Google on Disha Ravi, an environmental activist who was arrested for sharing a ‘toolkit’ to support farmers’ protests in India (Klein, 2021, as cited India-FoN, 2021). Although Ravi’s case is just one example, this illustrates data collection from SMPs as a method of dataveillance, which will be expanded upon in Subsection 6.2.1.1.

In summary, purchasing spyware from private companies, government funding of external operations, international collaboration, and data requests made to platforms illustrate both direct and indirect forms of -veillance operations in India. Together, these findings offer a comprehensive analysis of the socio-political landscape in the country. They further provide valuable insights into India’s engagement with -veillance technologies, their structural adaptations, and interactions among multi-stakeholder actors. Taking structural and agents links into account, the analysis provides insights into the triadic interplay of -veillance operations through technological lenses in the context of India.

6.1.2 United Kingdom

6.1.2.1 Government-Linked -Veillance Operations

Dataveillance through Regulation

For consistency, this subsection applies the same definition of dataveillance through regulation provided in Subsection 6.1.1.1. My FoN analysis identified two such regulatory practices leading to dataveillance in the UK: bulk data collection and through service providers.

The first form of dataveillance through regulation is bulk data collection by Britain’s intelligence agency, the Government Communications Headquarters (GCHQ). In 2013, Edward Snowden’s revelations⁶¹ exposed GCHQ’s interception

⁶¹ See Subsection 2.1.1 for more details on Snowden’s revelations found in the literature.

of international fibre-optic cables to gain access to phone calls, internet traffic, and social media posts (MacAskill *et al.*, 2013; MacAskill *et al.*, 2013, as cited in UK-FoN, 2016-2021). The literature situates these practices within post-9/11 security concerns in Western states (MacAskill and Dance, 2013). Furthermore, my data source triangulation from older FoN reports highlights that aspects of the UK and US's sharing of intercepted information were also in breach of human rights, as ruled by the Investigatory Powers Tribunal (Bowcott, 2015, as cited in UK-FoN, 2016). Although the legal framework surrounding this operation is reviewed in Subsection 6.3.2.2, bulk data collection continues to reflect the UK's direct gathering of data as a form of dataveillance.

The second form that dataveillance occurs as a result of regulation is through the practical powers vested in internet and mobile service providers. The UK regulates these actors through data retention and age verification (see Section 6.3.2 for my legal assessment). Moreover, my FoN analysis also revealed a case study in which 'two unnamed internet service providers' installed surveillance equipment under the Investigatory Powers Act (IP Act) (Burgess, 2021, as cited in UK-FoN, 2021). Although this may be viewed as a collaboration with two external actors, these methods underscore how the UK's regulations can lead to data collection.

Together, GCHQ's bulk dataveillance and data obtained from service providers comprise the UK government's regulatory mechanisms leading to its dataveillance operation. This form of operation shows how -veillance was integrated into the UK's structural framework and influences the ways in which agencies' data is collected.

Technical and Non-Technical -Veillance Operations

My analysis of FoN reports raised four technical and non-technical -veillance operations in the UK. To provide a detailed evaluation, I categorised these into two groups: routine and COVID-19 operations.

The first group of routine -veillance operations fall under SOCMINT, a social media intelligence method that monitors, collects, and analyses publicly available information on platforms. FoN reports highlight the work of Privacy

International, a UK-based NGO, regarding the UK's use of SOCMINT on activists (Privacy International, 2019, as cited in UK-FoN, 2021). To contextualise these findings, my targeted literature review identified additional examples showing that both the UK police and local authorities employ SOCMINT. For instance, South Yorkshire Police signed a two-year contract costing £55,000 for a SOCMINT tool in 2017 (Privacy International, 2020a). This case illustrates how externally developed surveillance technologies were structurally integrated into UK policing.

Another example is the Freedom of Information Act (FOIA) requests made by Privacy International, asking 136 local authorities whether they used SOCMINT. Their report revealed that 62.5% used 'overt', 31% used 'covert', 23.1% were not using overt methods, 5.9% were 'not clear', while 1.5% refused to respond (Privacy International, 2020b). To provide a distinction between these modes of surveillance, overt monitoring is one-time and causal, whereas covert is investigative, continuous, and legally requires a warrant in the UK (Privacy International, 2020b). Similar to the police example, the local authorities' use of SOCMINT illustrates their structural adaptation for conducting surveillance operations.

The second group comprises operations conducted during the COVID-19 pandemic, demonstrating the UK's use of digital governance at a time of crisis. Although there were concerns about the UK's data collection from service providers, like O₂ (Martin, 2020, as cited in UK-FoN, 2021), the government ran a two-year project called 'Test and Trace' as an attempt to control the disease's spread (GOV.UK, 2020). This technical project entailed dataveillance of text and calls, monitored movements to identify any contact with people who may be COVID-positive, and kept a record of some UK citizens' quarantine periods and COVID test results (GOV.UK, 2020). It is worth noting that the data collected under Test and Trace came under the UK's Data Protection Act (see Subsection 6.3.2.3), highlighting the legal basis to this operation.

The last COVID-19 operation I identified is a non-technical -veillance operation conducted by an army unit, the 77th Brigade. This finding emerged from a report

I deliberately triangulated following the FoN report's note on the Cabinet Office's establishment of a Rapid Response Unit (RRU) during the pandemic. The 'Ministry of Truth: The secretive government units spying on your speech' report by Big Brother Watch, a civil society organisation, revealed the RRU's collaboration with the 77th Brigade to monitor Twitter in the UK during COVID-19 (Carlo *et al.*, 2023). Although this will be discussed in more detail under my shaped discourse theme (see Section 8.1.2), it highlights the UK's reliance on military personnel in monitoring SMPs.

Overall, the UK's technical and non-technical operations reflect the government's response and adaptation to -veillance technologies at both normal times and crisis periods, like COVID-19. The use of SOCMINT by the police and the 77th Brigade not only demonstrates the policing and militarising of SMPs but also exposes the state control built into the UK's digital governance. Together, these operations illustrate how the UK has integrated -veillance technology to monitor and collect data about the public in its governance.

6.1.2.2 Government Collaboration with Other Actors on -Veillance

The government's collaboration with other actors illustrates its indirect conducting of -veillance operations, which also help us to comprehend other existing actors in the country. My analysis of the FoN reports identified three types of collaboration in the UK. These are international collaboration, integrating an externally developed programme, and collaboration with intermediaries, as discussed below.

The first is cooperation with other states to oppose encryption on SMPs. One key instance of this was when the UK's Home Secretary,⁶² alongside her counterparts from Australia and the US, wrote an open letter to Facebook opposing the platform's 'privacy first' plans to 'implement end-to-end encryption' in 2019 (Home Office, 2019, as cited in UK-FoN, 2019-21). Another example was when the Five Eyes group, which includes the UK, published a joint statement together with India and Japan, asking for 'backdoor access' to Facebook in 2020

⁶² Priti Patel was Secretary of State for the Home Department (2019-2022).

(Cimpanu, 2020, as cited in UK-FoN, 2021). Both these examples illustrate the government's formal collaboration to expand its -veillance access to Facebook.

The second type entails adopting an externally developed -veillance tool into the government. One example of this identified is Cardiff University's 'Online Hate Speech Dashboard' (or HateLab Dashboard). Established in 2017, the HateLab Dashboard received £1 million in funding⁶³ to develop an artificial intelligence tool for real-time monitoring and identifying of hate speech, to 'preempt hate crimes' being perpetrated on SMPs (BBC News, 2018, and Cardiff University, 2018, as cited in UK-FoN, 2019). Secondary sources confirmed its integration into the UK's National Online Hate Crime Hub and its use by the Welsh government to tackle hate speech (Osborne, 2023). Additionally, the developed tool was also used in collaboration with NGOs, tech firms like Google, and other governments including that of the US (Osborne, 2023). Altogether, HateLab exemplifies the role of government in financially supporting -veillance development, integrating it into government, and showing how the collaborated product contributes to the international dual-use market.

The final type of UK government collaboration is with intermediaries. This includes the example given on O₂ in the 'Technical and Non-Technical Operations' category, illustrating the government's collaboration with service providers. My research finding regarding SMPs as intermediaries will be discussed in detail in Subsection 6.2.2.1.

Overall, this section has provided an account of the government collaborations with other actors regarding -veillance by discussing international collaboration, integrating an externally developed programme, and collaboration with intermediaries. My analysis addressed directly and indirectly linked operations, identified types of tools and approaches used, and outlined key stakeholders within the socio-political landscape of the UK. The findings presented here offer insights from a technological perspective and show how the UK government has interacted with, and been shaped by, structure and agents. Following this

⁶³ Funded by the ESRC and the Alfred Landecker Foundation (UKRI, n.d.).

detailed examination of -veillance operations in my two case study countries, Part 6.2 focuses on the role of SMPs in -veillance.

6.2 The Role of Social Media Platforms on -Veillance

6.2.1 India

6.2.1.1 Transparency Reports

This subsection complements the finding introduced above on the Indian government's collaboration with my quantitative analysis of transparency reports from Facebook and Twitter. Doing so not only emphasises the multi-stakeholder environment of digital governance but also highlights the structure and established mechanisms SMPs have constructed. I did this by analysing the total number of requests, the number of accounts requested by the government, and the SMPs' compliance rate with these requests.

First, Figure 6.1 depicts the total number of requests the Indian government made to Facebook, which increased every six months between 2019 and 2021. During these three years, the government made the least number of requests, 22,684, in January-June 2019 and the highest, 50,382, between July and December 2021. In total, the Indian government made 220,899 requests, with an average of 36,814 user data requests every six months.

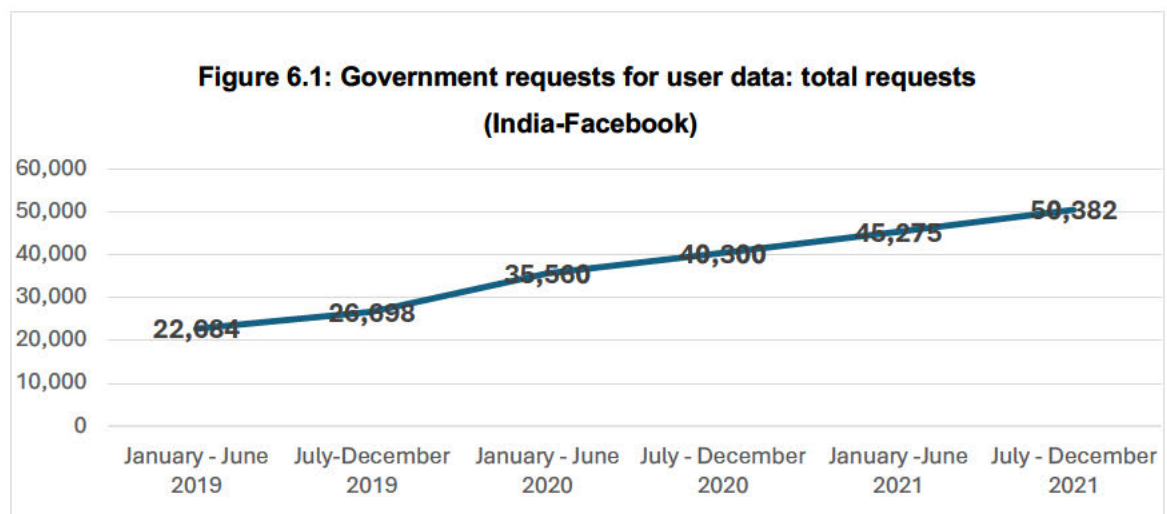
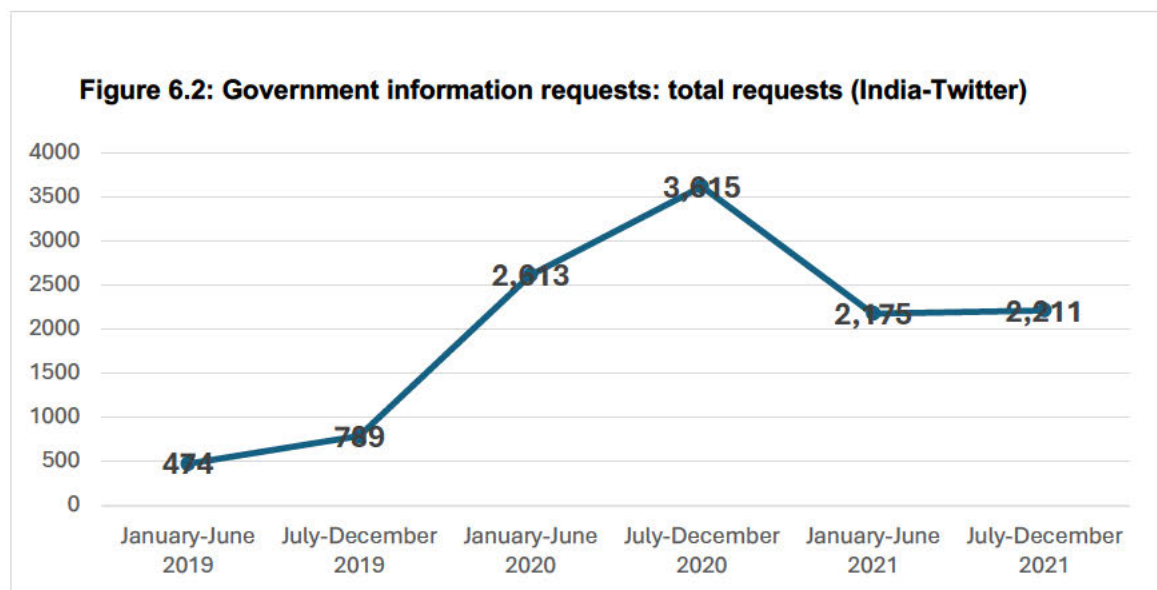


Figure 6.2 shows the Indian government's information requests to Twitter in the same period. Unlike Facebook, the number of requests varied and did not follow a consistent trajectory. The lowest number of requests was 474 in January-June 2019, while the highest was 3,615 in July-December 2020. Overall, the Indian government made a total of 11,877 requests in three years, that is, an average 1,979.5 requests every six months. These numbers illustrate the Indian government's interest in obtaining user data from these SMPs, complementing the dataveillance discussion in Subsection 6.1.1.2.



Second, I analysed the number of accounts the Indian government requested, which differed from the total requests, as some requests contained multiple accounts. Figure 6.3 depicts the number of total requests and the number of accounts the Indian government requested from Facebook. The evidence shows that both figures constantly increased every six months between 2019 and 2021. The lowest number of requested accounts was 33,324 between January and June 2019, while the highest was 81,501 between July and December 2021. In total, the Indian government made 220,899 requests to get data from 342,993 accounts on Facebook between 2019 and 2021, an average of 57,166.5 accounts every six months.

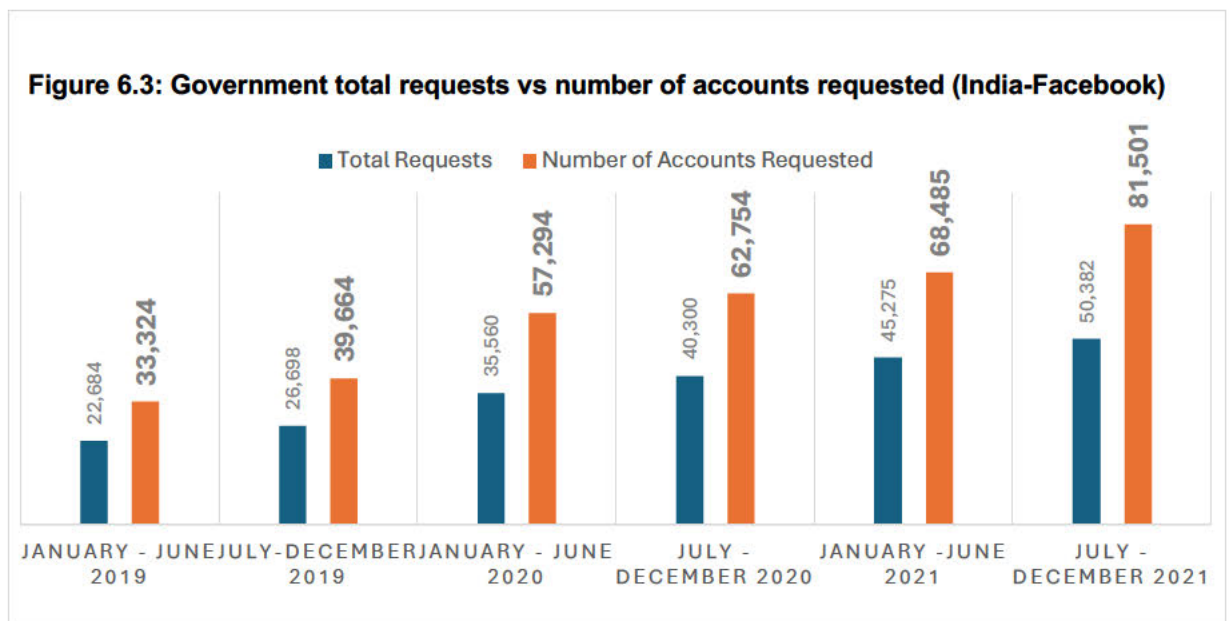
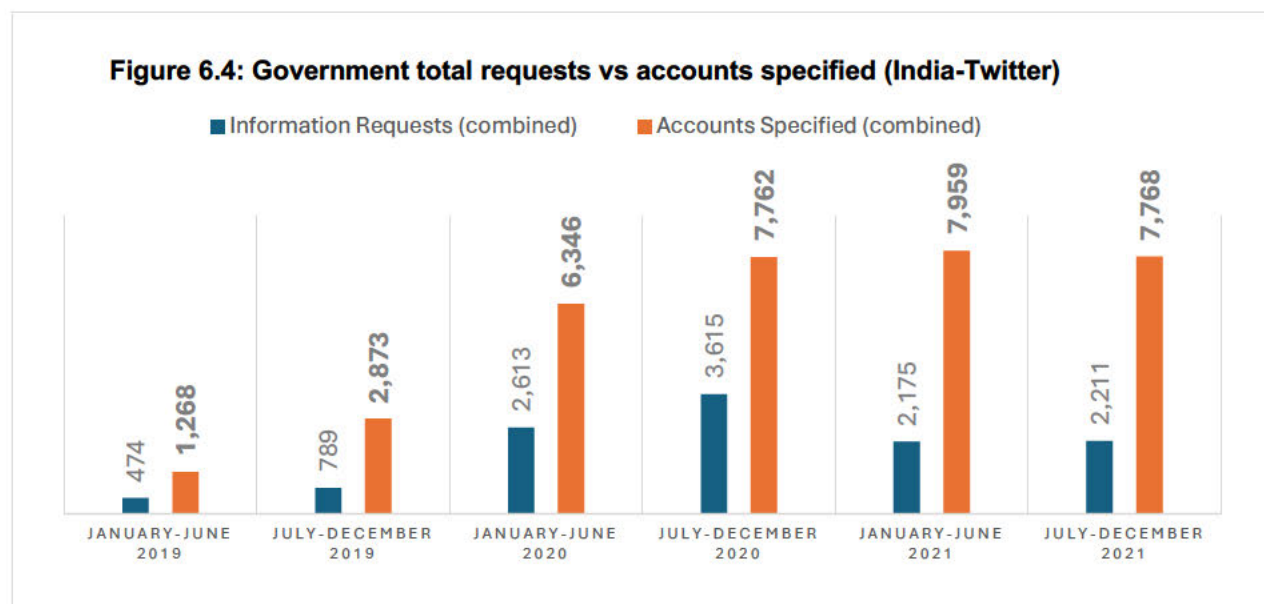


Figure 6.4 displays the total number of requests and the number of accounts the Indian government requested from Twitter, showing an unsteady pattern in the three years studied. The lowest number of accounts requested was 1,268 between January and June 2019, and the highest was 7,969 between January and June 2021. In total, the Indian government made 11,877 requests to obtain data from 33,976 specified accounts from Twitter, an average of 5,662.7 user accounts requested every six months. Highlighting the difference between the total number of requests and the number of accounts requested was important because it showed the government's mass requests and its reliance on the SMPs for user data, which is further evaluated by my respondents in the next subsection.



Third, I analysed the SMPs' compliance rates with the Indian government's requests. This was to understand how both platforms managed and responded to government requests within their own structure. Unlike the constant increase in the number of requests (Figure 6.1) and accounts requested from Facebook (Figure 6.3), Table 6.2 shows that the percentage of producing data - that is, user data - which Facebook gave the Indian government fluctuated. I found that Facebook complied least between January and June 2020 and most in July-December 2021, with an overall average compliance rate of 54%. I then applied this percentage to the number of user data requests made to Facebook. The result shows that Facebook shared 188,995 accounts data with the Indian government between 2019 and 2021.

Table 6.2: % of data produced from Facebook-India

India-Facebook (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July-Dec 2021
% of data produced	54%	57%	50%	52%	51%	64%

Figure 6.5: % data produced (user account) (India-Facebook)

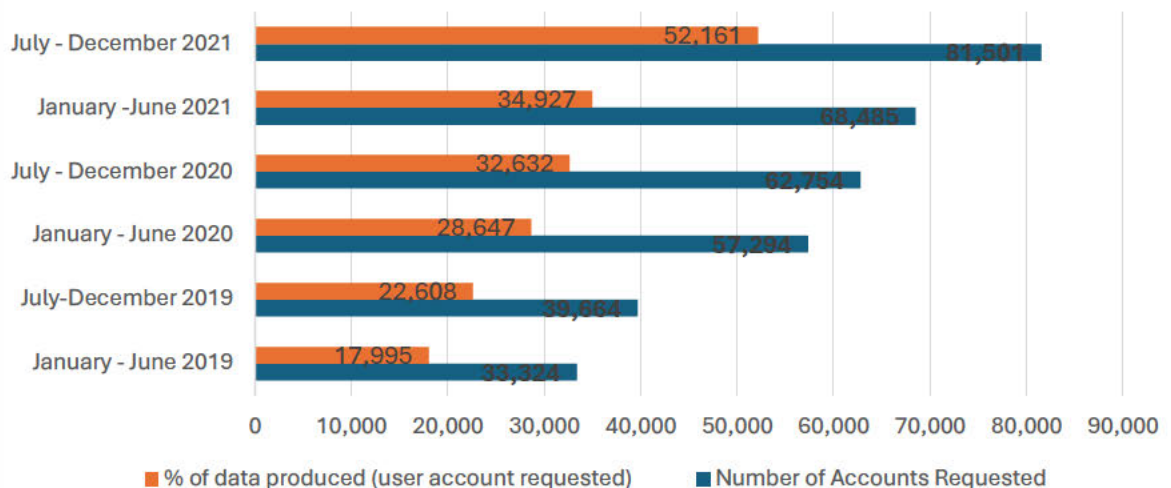
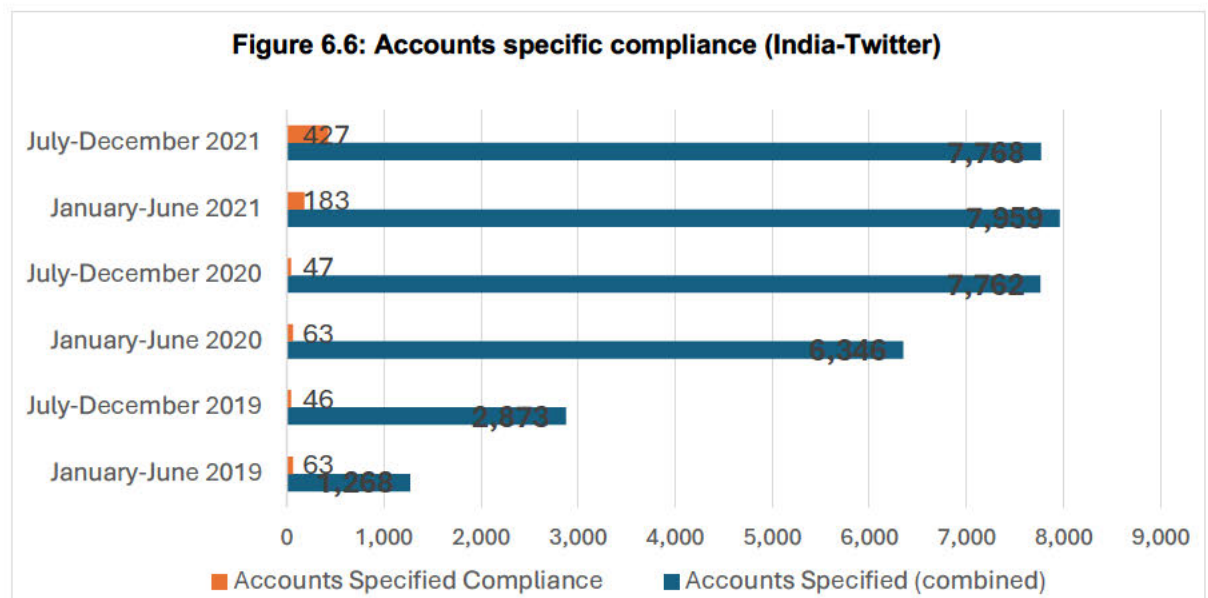


Table 6.3 portrays Twitter’s compliance rate with requests from the Indian government. Like the number of requests (Figure 6.2) and specified accounts (Figure 6.4), Twitter’s compliance rate was variable. Twitter complied the least in July-December 2020, and the most in July-December 2021, with an average compliance rate of 2.6% every six months. I then applied this compliance percentage to the number of requested accounts, as shown in Figure 6.6. Based on that, I determined that Twitter provided data on 829 accounts between 2019 and 2021. Analysis of both SMPs’ compliance rates with the Indian government’s requests shows that neither platform fulfilled all requests, underscoring the unique role of SMPs and their structural power to decide whether to comply.

Table 6.3: Compliance rate of Twitter-India						
India- Twitter (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July- Dec 2021
Compliance Rate (combined)	5%	1.6%	1%	0.6%	2.3%	5.5%



This subsection has analysed the two SMPs’ provision of user data to the Indian government by focusing on its total number of requests, number of accounts requested, and the compliance rate reported in the platforms’ transparency reports. In summary, Facebook received more requests for a higher number of

accounts and had a higher compliance rate than Twitter in India. Interestingly, both platforms' compliance rates were highest in the July-December 2021 period, which may have been influenced by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, which came into force in February 2021 (see Part 6.3 for more on this).

6.2.1.2 Assessing the Role of SMPs on -Veillance

This subsection supplements findings on the role of SMPs by presenting viewpoints derived from my interviews. I have categorised them into two points: concern about the availability of information on collected data, and the government's interest in obtaining the data SMPs' hold.

First, Karan underscored the role of SMPs through the public's reliance on transparency reports, which he found problematic:

So, the problem is that we rely primarily on reporting by the technology companies themselves because the requests are made by state police departments, so there's no aggregate level of data that exists in India. But I have noticed that there is an increasing trend of legal requests, so I've looked at stats by Google, Twitter and Facebook, or Meta, and I've seen that there's a steady increase in that.

Karan views the absence of a national database of government requests as something that creates 'reliance' on company reports, indicating a degree of dependency, control, and dissatisfaction. His reference to an 'increasing trend' and 'steady increase' situates legal requests as becoming popular in India. While this aligns with my Facebook analysis, my Twitter findings show an unsteady number of requests between 2019 and 2021.

Second, some respondents highlighted SMPs' role in holding information that is not available to the Indian government, but the government is interested in obtaining. One way this was discussed was through the Indian government's interference with Twitter's management to access the data. A policy director, Vikram, argued that 'a whistle-blower from Twitter, who testified to the Congress in the US [referring to Peiter Zatko], and he made certain suggestions about India, where he also said that there were potentially government agents

on Twitter’s payroll’. To validate this, I checked other secondary sources, which confirmed that the Indian government had ‘forced Twitter to hire an individual who was a “government agent” and likely had access to sensitive user data’ (The Wire Staff, 2022). Such interference with Twitter aligns with further insights gained from a security analyst, Nikhil:

The governments also put pressure on social media platforms to employ government agents at these platforms [...] To give a very specific example, during the farmer protests, the Indian government had an agent of theirs appointed on Twitter, who had the ability to look at the back-end information of several prominent accounts that were involved in the farmer protests and divulge information about who was behind them, which is both a clear violation of the privacy of these individuals on that platform but also raises important security risks for these individuals and their wellbeing as well.

Nikhil’s quote framed the government-platform relationship as coercive, implying the government’s attempt to control the platform and access the information they hold. His assertion of ‘agents’ being appointed to platforms like Twitter to obtain ‘back-end information’ indicates the government’s unauthorised intrusion into platform infrastructure. His comments about this, like ‘a clear violation of privacy’ and ‘security risks’, frame government actions as a threat for both the platforms and their users.

Both points about the availability of information regarding collected data and the government’s interest in obtaining SMP data assess the role of SMPs by comparing them with the government. This underscores my respondents’ acceptance of them as independent actors, while also providing insights about their role in -veillance management. Together, my analyses of transparency reports and interviews revealed how platforms interact with the government, offering a comprehensive examination of SMPs’ role regarding -veillance in India.

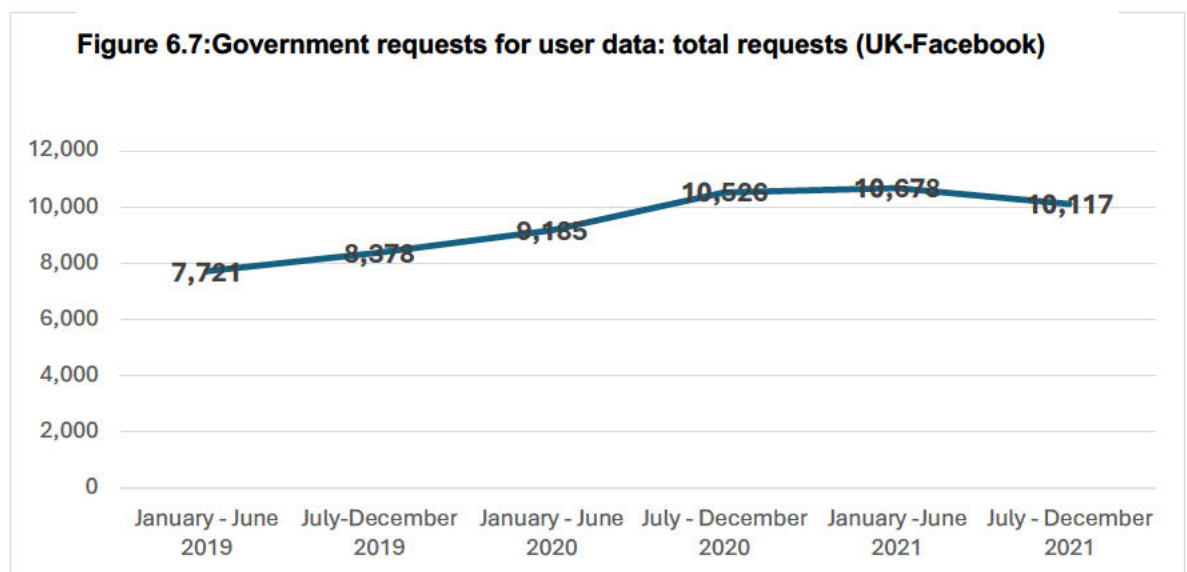
6.2.2 United Kingdom

6.2.2.1 Transparency Reports

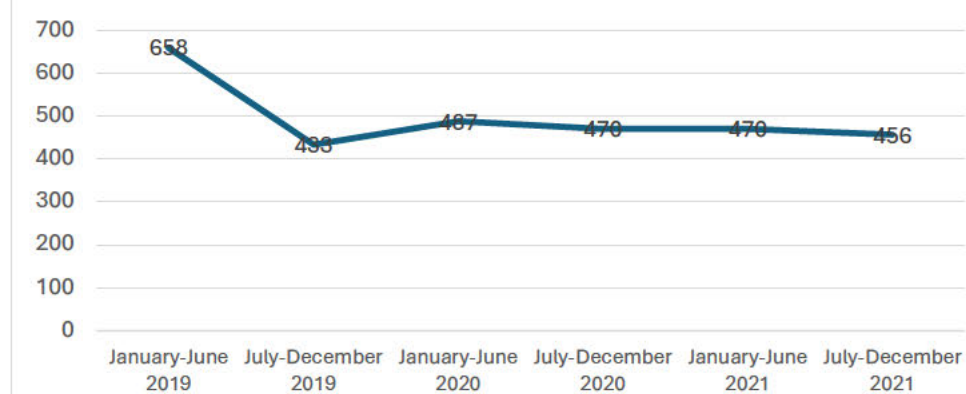
In line with my research purpose set out in Subsection 6.2.1.1, this subsection analyses transparency reports from Facebook and Twitter regarding the UK

government's user data requests. It examines the total number of requests, the number of accounts requested, and the platforms' compliance rates.

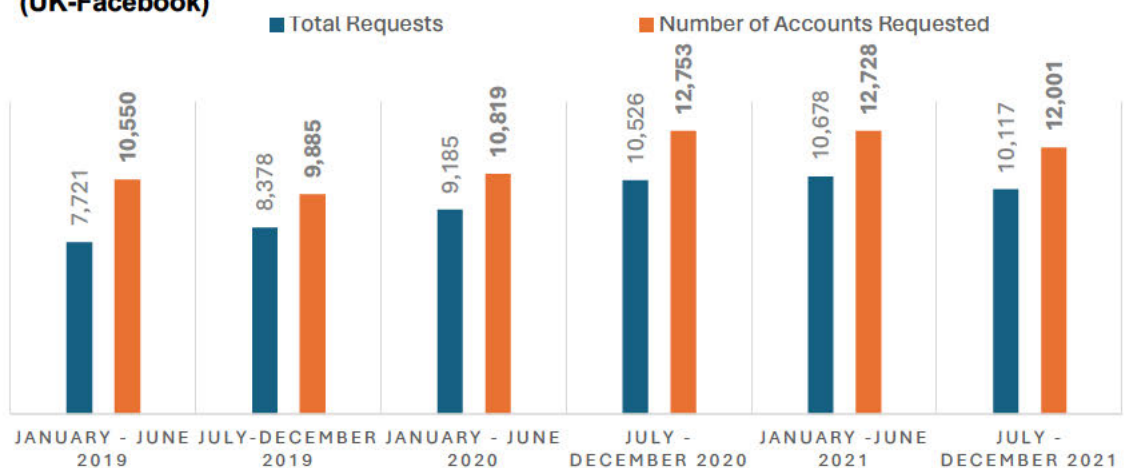
First, I evaluated the total number of requests the UK government made to the two SMPs, including routine, legal, and emergency requests. Figure 6.7 shows the number of requests to Facebook between 2019 and 2021. During those three years, the lowest number of requests was 7,721, in January-June 2019, while the highest was 10,678 in January-June 2021. This was a total of 56,605 requests, an average of 9,434.1 every six months.



Like Facebook, Figure 6.8 shows a pattern of unsteady requests from the UK government to Twitter. Between 2019 and 2021, the lowest number of government requests was 433 in July-December 2019 and the highest was 658 in January-June 2019. In total, the UK government made 2,974 requests in this period - an average of 495.6 every six months. These graphs depict the UK government's data collection from the two SMPs, providing supplementary data to the 'Government Collaboration with External Actors' detailed in Subsection 6.1.2.2.

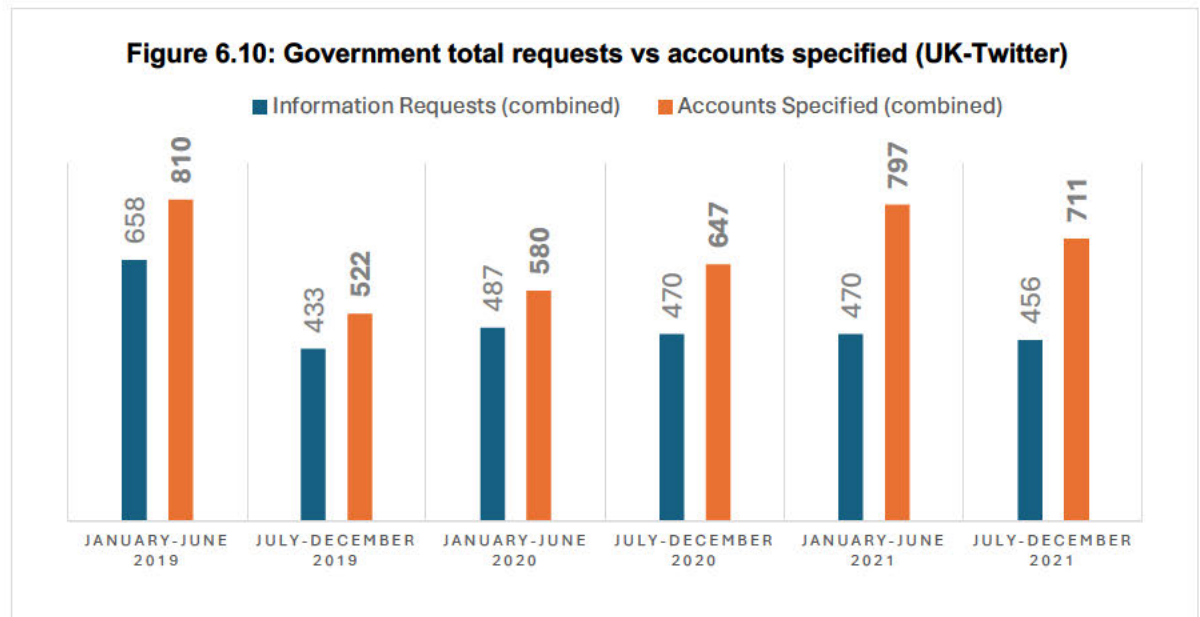
Figure 6.8: Government information requests: total requests (UK-Twitter)

Second, I analysed the number of accounts requested. Figure 6.9 shows that the UK government requested more accounts than the total number of requests made to Facebook between 2019 and 2021. Within those three years, the lowest number of accounts requested was 9,885 during July-December 2019, while the highest number was 12,753 between July-December 2020. In total, the UK government made 56,605 requests to get 68,736 accounts from Facebook, an average of 11,456 account requests every six months.

Figure 6.9: Government total requests vs number of accounts requested (UK-Facebook)

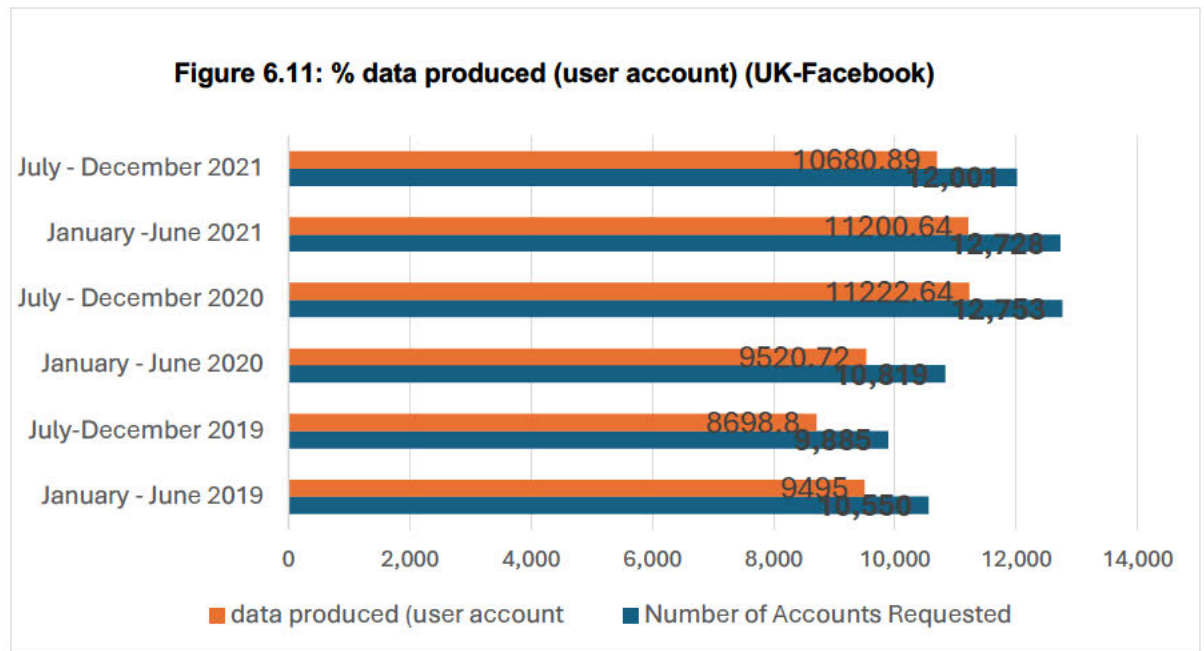
In contrast, Figure 6.10 shows the number of accounts the UK government requested from Twitter. The lowest number of accounts requested was 522 during July-December 2019, while the highest number was 810 during January-

June 2019. The UK government made a total of 2,974 requests for 4,067 accounts - an average of 677.8 accounts every six months. By highlighting the difference between the number of requests and the number of accounts requested from the two platforms, my analyses provide numerical data on the government's reliance on the platforms themselves for information about SMP users.



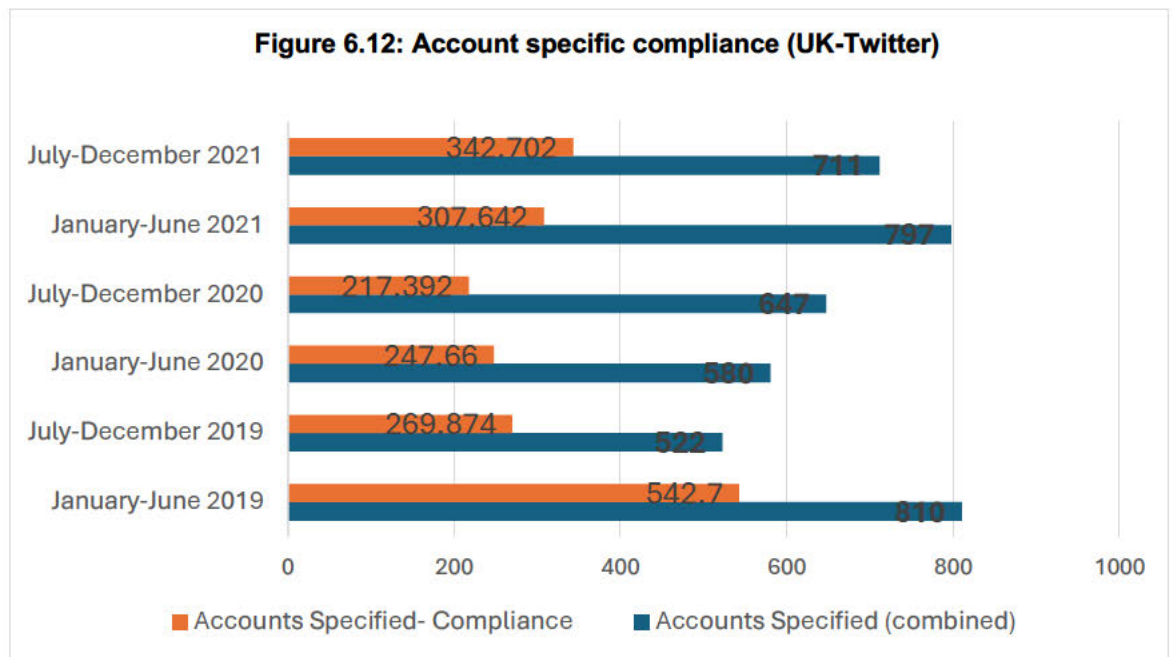
Third, I examined the SMPs' compliance rate with these government requests to ascertain the amount of user data they provided in response. As Table 6.4 shows, the percentage of data produced from Facebook was relatively high. In the three years of my research, Facebook had the lowest rate of compliance, 88%, in two periods: July-December 2019 and January-June 2021, and the highest, 90%, in January-June 2019. This made an average compliance rate of 88.5%. I then applied the compliance percentages to the number of requested accounts to further assess how much data Facebook had provided to the UK government. As set out in Figure 6.11, I found that Facebook had provided data about 60,815 accounts, out of 68,736 requested, to the UK government between 2019-2021.

Table 6.4: % of data produced by Facebook-UK						
UK -Facebook (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July-Dec 2021
% of data produced	90%	88%	88%	88%	88%	89%



In comparison, Table 6.5 shows Twitter's compliance rates, revealing that the lowest was 33.6% between July-December 2020, while the highest was 67% in January-June 2019. Twitter's average compliance with the UK government's requests was 46.9% between 2019-2021. I applied these compliance percentages to the number of accounts requested by the government, as shown in Figure 6.12. I found that Twitter provided data about 1,924 accounts out of the 4,067 requested by the UK government between 2019 and 2021. These findings offer insights into the UK government's reliance on SMPs, while also highlighting the platforms' role and power in deciding whether to comply with these requests.

Table 6.5: Compliance rate of Twitter-UK						
UK- Twitter (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July- Dec 2021
Compliance Rate (combined)	67%	51.7%	42.7%	33.6%	38.3%	48.2%



This subsection has analysed the total number of user data requests, the number of accounts requested, and compliance rate from Facebook and Twitter in the UK. When compared, my analysis shows that the UK government requested more user data and had a higher compliance rate from Facebook than from Twitter. This has not only complemented my analysis on government collaborations with SMPs given in Part 6.1 but also provided an analytical lens through which to examine the role of SMPs through government data requests.

6.2.2.2 Assessing the Role of SMPs on -Veillance

This subsection supplements the above quantitative analysis with qualitative data derived from interviews, reflecting on the role of SMPs. It addresses my UK respondents' views on the government's dependency on SMPs for data, and the cost of using SMPs for individuals.

First, one of my research respondents, Jessica, highlighted the UK government's dependency on SMPs for data collection. She framed this dependency as problematic, since SMPs were in a position where they could blackmail governments over data:

They would say, 'Oh well, we have this data, but you wanted to legislate this and this against us. So why don't we give you this data? But at the same time, you will be a bit more lenient when you're going to do that law against us,' right?

Jessica's opinion suggests that the government faces pressure to maintain a positive relationship with platforms while trying to ensure they are regulated and governed. The language she used positions SMPs not just as service providers but as actors who can use data strategically. Jessica further argued that these negotiations might not always be apparent and visible to the public: 'they are not transparent, so we don't really know, they are happening in the back end'. Her view reflects wider public opinion findings by Office for National Statistics, showing that only 34% of UK adults believe the government regulates emerging technologies responsibly (ONS, 2024). Together, these findings highlight a widely held perception of limited transparency and trust in the government's ability to effectively regulate platforms and other emerging technologies in the UK.

Second, some respondents challenged the assumption that social media is cost-free. As Richard commented, 'there is no such thing as free lunch [...] social media is not free, we're paying for it by selling our data'. Recognising SMPs' power over users' data, Richard interpreted the platforms' user data collection as a form of payment for using their services. He further argued that this data-driven 'business model' has negative impacts for both people and governments:

So, it's a lose-lose situation in my view, you've lost because of the company's use of the technology and when governments then begin to embark on the same thing, you have digital authoritarianism on a very grand scale.

Richard's use of the phrase 'lose-lose situation' constructs a pessimist view, framing citizens as victims of both platforms and governments. By invoking 'digital authoritarianism on a very grand scale', he sees governments and platforms' practices as a threat to democratic governance. From a different perspective, Mark pointed out that, 'at least the government, in theory, is supposed to be answerable to you and to me, Elon's not answerable to either of us'. Unlike Richard, Mark highlighted SMPs' independency of SMPs as a risk when compared to the government. He cited 'Elon Musk' as example to situate how

powerful SMP actors can be in digital governance. These viewpoints explain SMPs' power to not comply with all requests made by the UK government.

Both viewpoints on the government's dependency on SMPs and their cost to users emphasise SMPs' role in -veillance through their relationship with the government. Overall, this section has highlighted the key role and power SMPs hold in digital governance, by shedding light on how these platforms act as structures and as agencies, shape their own data collection mechanisms, and co-construct a digital governance system when interacting with governments' data needs. Taken together, these dynamics illustrate SMPs' distinctive position within digital structuration, demonstrating how they uphold their own structure, agency, and technology, while simultaneously interacting with other elements across the triad.

6.3 The Legal Frameworks on -Veillance

6.3.1 India

6.3.1.1 Individual Rights in Relation to -Veillance

This subsection examines individual rights in relation to -veillance, discussing citizens' capacity to act and be protected under the law in India. My analysis of the FoN data highlights two key individual rights: the right to privacy and the right to information requests.

First, the right to privacy has recently been recognised as a fundamental right in India. Although it was not originally included in the Indian Constitution, the Supreme Court declared the right to privacy as part of the right to life and liberty under Article 21 in 2017 (*Justice K S Puttaswamy (Retd.) v. Union of India*, W.P.(C) 494/2012, as cited in *India-FoN*, 2017-21). While this landmark decision shows India's expansion of individual rights into the digital sphere, Article 21 is not an absolute right and may be subject to legal exemptions (the Indian Constitution, 1950). This limitation demonstrates the extent to which the right to privacy is protected in India.

Second, India upholds the right to information requests under the Right to Information Act (2005) (RTI Act). This enables citizens to request government-held information as a form of data collection that enhances transparency in governance. Despite this agency empowering principle, Article 8 of the Act limits disclosure of information to the public for various reasons, including where disclosure would affect sovereignty, integrity, or the interests of the state (the Right to Information Act, 2005). This limit underscores people's capacity to obtain information from the government.

What emerges from my analysis of the right to privacy and the right to request information is that, although these rights are intended to protect and enhance citizens' capacity to act regarding -veillance, they are subject to limitations which mean that both rights can legally be infringed under existing frameworks.

6.3.1.2 State Legislation Governing -Veillance

My FoN analysis identified three key legislation and their allied rules that play a central role in regulating -veillance and provide information about India's legal structure in India. These are the Indian Telegraph Act, the Information Technology Act, and the Digital Personal Data Protection Act.

First, the Indian Telegraph Act (1885) plays a significant role in interception practices in India. The absence of any explicit definition of communications technology in its Section 5 allows the law to remain applicable to digital regulation and permits the government to intercept telecommunications for varied reasons (the Indian Telegraph Act, 1885). However, the expansive list outlined in this provision creates ambiguity and risks political interpretations and security rationales for interception, as seen in the parliamentary questioning of the Ministry of Home Affairs about Pegasus, detailed in Subsection 6.1.1.2.

Despite the continuous application of such an old law, India has developed its interception practices in newer legislation allied with the Indian Telegraph Act. For instance, the Indian Telegraph Rules (1951) set procedural limits on the government's interception, setting a mechanism for its practices (India-FoN, 2019). During my research period, India was working to replace the Indian

Telegraph Act with the Telecommunications Act, which was enacted in December 2023. Prior to this, my respondent Vikram had criticised the Telecommunication Bill's definition of 'telecommunication services':

They made it much broader, which also then includes messaging applications, saying 'you need a licence to operate', which potentially can mean that, like WhatsApp and Signal need to get licenced by the government to operate, and a condition of that licence is that you have to intercept messages.

To validate Vikram's concerns, I reviewed the Telecommunications Act (2023) and identified two relevant provisions he had raised about the law. Section 3 requires telecommunication providers to obtain 'authorization' from the central government, while Section 20 allows the government to possess and access messages on telecommunication services and suspend the transmission of communications for emergency and public safety reasons (Telecommunications Act, 2023). Despite Vikram's concern, the legislation retains government authorisation, licensing, data collection, and the power to interfere with communications at times of emergency or when public safety is jeopardised.

Second, the Information Technology Act (2000) (IT Act) and its two allied rules outline the main legal frameworks regarding the governing of -veillance. The IT Act (2000) plays a critical role in interception and decryption practices in India. One of the most prevalent sections that emerged from my analysis is Section 69 of the Act. This provision outlines legal justifications for interception, provides grounds for government access to data, covers government assistance in decryption, and threatens firms with up to 7 years imprisonment if they fail to comply (the Information Technology Act, 2000). The broad and vague definition of this provision makes access to data susceptible to political misuse and creates direct regulatory pressure on intermediaries and their decryption operations.

Adapting to technological developments, the Information Technology (Amendment) Act (2008) extends the IT Act's frameworks to surveillance and dataveillance on computers (India-FoN, 2019). Specifically, Sub-section 69.B of the Act authorises monitoring and data collection from computers for security reasons. It outlines the monitoring process, including intermediary assistance

and data processing procedures, and states a jail sentence of up to three years for non-compliance (see the Information Technology (Amendment) Act, 2008). This amendment parallels Section 69 of the IT Act (2000) and reinforces state pressure on intermediaries by extending the scope of legal jurisdiction to include computers.

Following the growing dominance of platforms, India developed the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules in 2021, which made key changes in the governance of SMPs. The Rules imposed stricter data retention and compliance requirements on intermediaries, including a 72-hour rapid compliance limit and the need to store information for 180 days (Section 3.1.g of the IT Rules, 2021). They also addressed the conflict about the decryption of the first originator, which clashed with service providers' use of end-to-end encryption (India-FoN, 2019). Sub-section 4.2 resolved this by empowering authorities to request decryption for various reasons (IT Rules, 2021). This legal pressure to break encryption resulted in Facebook and WhatsApp filing petitions with the Delhi High Court (Agrawal, 2021). Their response offers insights about the triadic engagement between government regulation, platforms, and user data, as well as platforms' reliance on domestic jurisdiction to resolve issues arising from this. Altogether, the IT Act and its allied laws illustrate how legal frameworks around monitoring, data collection, and decryption have been constructed over time in India.

Third, the Digital Personal Data Protection (DPDP) Act (2023) marked India's first personal data protection legislation. My FoN analysis examined the Act's historical evolution. First drafted in 2018 (India-FoN, 2018-9), the Bill followed a public consultation process, noting concerns about expanded government power and privileges, and criticism of the proposed data localisation model due to security and surveillance risks (Bhandari, 2019, Bailey, 2020, and Basu and Sherman, 2020, as cited in India-FoN, 2021). To ensure a valid analysis of these presumptions, I examined the enacted legislation.

Broadly, the DPDP Act (2023) establishes a comprehensive legal framework for the collection, processing, and defining of structural powers on data. It created

new bodies, such as a Data Fiduciary, Data Processor, and Data Protection Officer, as well as a Data Protection Board, which empowers the central government by obtaining and decoding data (see Chapters 5 and 6 of the DPDP Act, 2023). Regarding citizens' rights, the Act gives Data Principals (individuals whose data has been collected) the right to be informed about the processing of their data; however, this is a limited right (Section 11 of the DPDP Act, 2023). Moreover, although the Act did not propose a data localisation model as discussed in the FoN reports, Section 16 focuses on the processing of data outside India under the control of the central government (the DPDP Act, 2023). Overall, the Act demonstrates how India has shaped its first data protection framework by combining personal rights with a centralised governance.

Taken together, these three laws - Indian Telegraph Act, the Information Technology Act, and the Digital Personal Data Act - illustrate how India's state legislation on -veillance was constructed and shaped by technological mandates over time. My analysis shows that they regulate technology, service providers, and citizens' data, which collectively offer insights for a triadic interaction from structural perspectives. Following this state-based analysis, the next subsection considers the legal concerns my respondents raised.

6.3.1.3 Legal Concerns About -Veillance

Opinions about the functioning of judicial and legal systems vary in India. Existing data from 2019 show that 47% of Indians believe the court system treats everyone fairly (Devlin, 2019). While this indicates that less than half of Indians express confidence in judicial fairness broadly, this subsection presents three specific legal concerns derived from my Indian respondents in relation to -veillance. These relate to the consultation periods of proposed legislation, state-centric regulation, and the DPDP Bill.

The first concern that emerged regarded the inefficiency and procedural distrust of public consultations during law-making. Sanjay argued that:

[...] the Indian Telecommunication Bill 2022, which has been used for public consultation two days ago. It is sweeping in terms of the kind of power that it gives the government with absolutely zero oversight, either

judicial or legal, or parliamentary oversight. There is no checks and balances in place [...] it gives government immense power to direct any company to disclose messages, to stop any transmission of messages [...].

Sanjay's observation reflected his surprise at how the government-empowering Bill was prepared and subsequently opened for consultation. In a way, he framed this as a dilemma in which a seemingly democratic process of consultation was used to legitimise an extreme form of power centralisation in the government. Similarly, Vikram commented on the consultation period for the IT Rules (2021):

The government will argue that they did a consultation process back in late 2018. [...] if you look at the IT Rules that came out, they were very different from the ones that were put up for public consultation [...] Since then, the general narrative is that 'hey, in India we want safe, accountable, open, transparent internet', that's their terms that they use. But what exactly do these terms mean? Sometimes for the sake of having a consultation process they put out a document, leave it open for a month for people to respond to with public comments, and then you don't hear about it for sometimes months, sometimes years, until they suddenly decide to notify it. And during this process they never put out the responses that people gave, so you don't even know how different people have responded [...].

Vikram's reflections on the consultation period framed the process as a formality rather than a democratic approach. While his observation that 'they were different from the ones that were put up for consultation' could point to the marginal changes made to the Bill during the legislative process and raises questions about whether the consultation process was as 'transparent' as claimed. Both Sanjay and Vikram's views on the consultation periods raised aligned concerns about how legislation is crafted and the extent to which the public can effectively participate in law-making.

The second concern raised was the government's state-centric regulation of -veillance. Amit asserted that the problem stemmed from either 'bad-shaped' laws or the lack of regulations 'that govern data privacy, use of media' in India. But either way, he argued that:

And they don't essentially adhere to the principles of regulation in terms of protecting the voice, or freedom of speech, or rights of citizens, or privacy or data protection of citizens, so they don't really adhere to the

fundamental principles of those. But in the name of those principles, they generally most often protect the interests of the ruling dispensation.

Amit framed a duality in how good intentions behind laws and principles can also be politicised in practice. This was supported with an example from Vikram, who asserted that the law has created a deadlock between intermediaries and users' right to privacy:

Realistically, there's no way to implement that without compromising end-to-end encryption [referring to the provision on the first originator, see Subsection 6.3.1.2]. Now the government is saying, 'hey we're not saying break encrypting, we are saying tell us who sent the message'. I think that's a little disingenuous if you understand the technology and how it works because it's not possible to that. But interestingly, both Facebook and WhatsApp have challenged that requirement in court.

Vikram reflected on how the Indian government uses the law to legitimise breaking 'end-to-end encryption' under the 'first originator'. Although both terms require breaching users' privacy and disclosing their data, his point addressed a narrative that exploits technical capabilities and puts platforms under significant pressure. Together, these views underscore the dual character of laws, highlighting how their practical and operational effects can diverge.

The third concern my respondents raised was during the Bill phase of the DPDP Act. To ensure the validity and credibility of their assessments (which were made before its enactment), I describe their concerns and then review the enacted provisions of the DPDP Act (2023) below.

First, Manish emphasised the importance of a regulatory gap the DPDP Act would fill, since 'all privacy related laws were organisation-centric'. Although it was India's first law on personal data protection, my analysis set out in Subsection 6.3.1.2 illustrated its comprehensive scope, going beyond simply safeguarding citizens' rights. Second, Arjun deemed the Bill to be important due to its definition of digital personal data: 'the Bill is only going to be advocated to digital personal data, which is any data which is collected online and any offline data which has been digitized'. This is ratified under Section 3 of the Act (2023), which specifies the processing of data collected: '(i) in digital form; or (ii) in non-digital form and digitized subsequently'. Third, Karan commented that the

Bill was important because of ‘political parties’ use of data from social media platforms and other sources to engage in electoral politics’. This would have been politically problematic and challenging to Indian democracy if implemented; however, the Act does not contain any such provision on the use of data by political parties or during elections⁶⁴.

This subsection has analysed concerns my respondents raised about consultation periods of any proposed legislation, state-centric regulation, and the DPDP Bill, in relation to -veillance in India. Drawing links to existing frameworks, it has highlighted the language framing how these regulations and legislation are state-centric, creating problems for both SMPs and individuals. Such a complex influence of the law within digital governance demonstrates its interplay with the platforms and Indian citizens.

6.3.2 United Kingdom

6.3.2.1 Individual Rights in Relation to -Veillance

To understand citizens’ legal capacity to act and be protected in the digital sphere, this subsection reviews two democratic rights in relation to -veillance in the UK. These are the right to privacy and the right to request information, as presented below.

First, the UK grants citizens the right to privacy under the ‘right to respect private and family life’ set out in Article 8.1 of the Human Rights Act (1998). However, Sub-section 8.2 of the same Act notes that this right can be subject to exemption (Human Rights Act, 1998). This demonstrates limitations on the extent to which individuals’ right to privacy can be protected and practiced in the UK.

Second, the UK guarantees individuals the right to request information, which resembles a form of data collection at the agency level. Citizens of England, Wales, and Northern Ireland have the right to request information under the

⁶⁴ I read the title of the provisions and a keyword search on ‘political parties’, ‘political’, ‘parties’, ‘election’, and ‘campaign’.

Freedom of Information Act (2000), as do Scottish citizens under the Freedom of Information (Scotland) Act (2002). While this foregrounds the devolution of states and their influence on digital governance structures, both Acts contain exemptions that restrict people's access to certain information in their Part Twos. In parallel with the right to privacy, this exemption illustrates a limitation on citizens' capacity to act in requesting information from the government.

Overall, the limitations on these privacy and information rights demonstrate that they are qualified rights, subject to restrictions imposed by other legislation. While this illustrates the legal landscape from the perspective of agency, it also underscores the complex interaction of the law with other aspects of digital governance.

6.3.2.2 State Legislation Governing -Veillance

This subsection reviews three laws I thematically identified from my analysis of FoN data to explain the UK's existing regulatory framework. These are the Regulation of Investigatory Powers Act, the Investigatory Powers Act, and the Data Protection Act.

First, the Regulation of Investigatory Powers Act (2000) (RIPA) is important for surveillance operations in the UK, providing the legal basis for Snowden's revelations on GCHQ's operations (see Subsection 6.1.2.1). It empowers the Home Secretary or the Foreign Secretary to sign bulk⁶⁵ interception orders on communication data, lists authorities who may perform covert and overt intelligence operations, and established the Investigatory Powers Tribunal to oversee its practices and address complaints (MacAskill *et al.*, 2013; UK-FoN, 2019). Despite its long-term effect, the European Court of Human Rights ruled bulk interception under RIPA to be in violation of the European Convention on Human Rights for reasons including the right to privacy, free expression and inadequate protection of journalists in 2018 (European Court of Human Rights, Case of Big Brother Watch and Others v. The United Kingdom, 2018, as cited in

⁶⁵ See Section 6.2.1 for the definition.

UK-FoN, 2019). However, the Court applied the ‘margin of appreciation’⁶⁶ doctrine (Justice Initiative, 2012; Privacy International, 2018, as cited in UK-FoN, 2019), which allowed the UK discretion in domestic issues and enabled RIPA to continue legalising bulk interception.

Second, the Investigatory Powers Act 2016 (IP Act) consolidated powers of ‘interception, equipment interference, and data retention’ under a single law (UK Home Office, 2016, and Investigatory Powers Act, 2016, as cited in UK-FoN, 2019). My data source triangulation of FoN 2016 provides a temporal context in which the Act emerged following the Investigatory Powers Tribunal’s ruling that existing operations at GCHQ had breached human rights law (UK-FoN, 2016). One of the ways the IP Act resolved this was by formalising procedures for data retention under its Section 87 and establishing oversight mechanisms, including the Investigatory Powers Tribunal (IP Act, 2016). However, the Act also restricts transparency over operational warrants under Section 57, which prohibits making ‘unauthorised disclosures’ (IP Act, 2016). This means citizens may not always be aware of the data that is collected and retained about them. For the regulation of operations, the Act distinguishes between international and domestic operations. It requires authorities to obtain targeted warrants for domestic operations, while international operations involve communication data, including bulk interception, acquisition of the communication data, and ‘bulk equipment interference’ (UK-FoN, 2019). This distinction upholds democratic safeguards domestically but means weaker protections internationally.

Third, the Data Protection Act (DPA) (2018) is the primary legislation for the protection and processing of personal data. It served as the national implementation of the European Union’s General Data Protection Regulation (GDPR) prior to Brexit. The DPA defines personal data, establishes its regulatory scope, and creates a special category of a data framework for processing such sensitive data under specified circumstances. It also grants data subjects’ rights, like the right to rectification or erasure, ensuring some individual control over

⁶⁶ The ECHR doctrine developed to address possible differences in the interpretation of certain issues across states (Justice Initiative, 2012).

their data (DPA, 2018). In summary, the Act provides a comprehensive framework governing dataveillance operations, the processing of collected data, and individuals' control over that data. Acknowledging its central role, my data source triangulation shows that legislators showed some signs of expanding their work when they introduced the Data Protection and Digital Information Bill in 2022, however, this was later withdrawn in 2023 (House of Commons Library, 2023). This illustrates both the UK's continuous adaptation to changing digital demands, and political contingencies shaping frameworks around -veillance.

The legislation analysed above - the Regulation of Investigatory Powers Act, the Investigatory Powers Act, and the Data Protection Act - provide essential insights into the legal frameworks surrounding -veillance in the UK. This section has encompassed how law codified the use of technologies, the regulation of communication services (including SMPs), and the governance of personal data. The changes and developments noted in the laws analysed above reveal how the UK adapts its legal structure to evolving technologies while seeking to protect its citizens. This analysis of the legal frameworks provides contextual information about structure and its triadic engagement with technology and agency.

6.3.2.3 Legal Concerns About -Veillance

This subsection discusses two legal concerns related to -veillance that emerged from my interviews. Before addressing these thematic insights, I will first incorporate public opinion data on trust in the courts to provide a general contextual background to the UK. According to the Office for National Statistics, 62% of people reported a medium to high level of trust in the courts and judicial system in 2023 (ONS, 2024). Despite this relatively high level of trust, this subsection examines the multiple uses of laws and data management in the UK.

The first concern my respondents raised was that the same law was being used for different purposes. According to Mark:

I think the problem is that, at the same time, as in the government, there are people trying to solve the problem, there are other people trying to use the same laws to increase surveillance or have an attempt at other things.

The language Mark used about the use of law underscores its dual effect: while it protects people and preserves national security through interception, it also raises security implications for individuals' data and privacy.

The second concern was the inadequate protection of individual rights and data under the law. Jessica argued that there is a problem with legal enforcement:

So, we saw that the Tory Party illegally targeted people during elections, and the ICO found them guilty [referring to Cambridge Analytica scandals], but they didn't really punish them. So, there are laws that exist, a lot of them are related to the GDPR. [...] they have kind of close connections with a lot of these social platforms. [...] it's kind of quite toothless, and then they're not really afraid of that. [...] if I want to sue Facebook, for example, like Max Schrems did with his organisation. [...] It took him four and half years to get any kind of ruling. So, if I want, as a citizen, to do something like that, it will take me years. So, then it's not only about legislation, it's about lacking enforcement that is not really helpful for citizens; [...] then the punishment is so little. Then how would these platforms be deterred from doing wrongdoings to citizens in this way?

Jessica framed legal enforcement as ineffective. Her examples of the Cambridge Analytica and Max Schrems cases illustrate both a systematic failure to enforce punishment and individual struggles over personal data, leaving citizens unprotected. From a different point of view, Mark asserted that GDPR lacks any data ownership for users:

[...] GDPR is just one element in a jigsaw of different regulations. So, GDPR is talking about your rights as an individual over your data. Now I get accused of being simplistic sometimes, but my view of this is 'you own your data', and people quite rightly point out, while GDPR doesn't mention ownership, but the rights that you have are very similar to ownership. [...] example I quite often use is lending a car. So, if you own a car, you lend it to me. I should not then lend it to someone else. And if I do lend it to someone else and they crash it, I should be responsible to you and not say 'Well, I don't know, there's some other guy I rented to crashed it'. So, it's only really your data and how it's used. Whereas, then, there needs to be a lot of other areas that we look at for social media and make sure that social media is included in all the laws about libel, laws around racist content, sexist content, all of those things. So GDPR is never enough.

Mark's 'car lending' example highlights the problem of platforms failing to take responsible care of the personal data they collect. His description of GDPR as only a part of other necessary legal frameworks that should be there can further be expanded on by Lauren's remarks:

GDPR, which was the European mechanism for managing usage of data, it does feel a bit like a David and Goliath when you think of the global reach of platforms like Facebook and the degree to which they are selling on our data quite happily for commercial ends. And obviously, the expert on this would be Shoshana Zuboff, who perfectly pretty much sums up exactly what's going on, and I don't think that any legislation has really changed the overall picture in respect of our lack of privacy and exploitation of our data for all sorts of different ends. However, I don't think that's the full story either, and I do wonder whether state governments haven't intervened more in that or being more perhaps some attacking it with a kind of stronger force, because at the end of the day they really don't want to interfere in the market, and that's not something state governments are interested in doing.

Lauren's use of the David and Goliath metaphor highlights the imbalance between users' lack of control over their data and the profit-oriented platforms, framing GDPR as insufficient. Her questioning of state control over data and her emphasis that 'they really don't want to interfere' and 'that's not something state governments are interested in' illustrates a critical view of the government's reluctance to challenge platform power.

Overall, this subsection has presented my respondents' legal concerns in relation to -veillance, raising the interplay of law with both platform regulation and its influence on individual rights. These concerns highlight the need not only for more citizen-centric data protection legislation, but also for stronger enforcement mechanisms.

6.4 Experts' Concerns and Views on the Implications of -Veillance on the Public

6.4.1 India

6.4.1.1 Awareness

My findings about awareness reflects the public's understanding of existing -veillance operations. My interview analysis shows a consensus among my respondents that awareness of -veillance in India was low. I have categorised their evaluations into two: the understanding of data in the country, and limited transparency.

First, some of my respondents explained that awareness was low due to the country's general understanding and perceptions of data. Nikhil argued that 'the value of data privacy and individual data is not as high as it might be in other places due to a lack of equal distribution of education and socio-economic opportunities'. Although Nikhil framed this problem in terms of education and socio-economic inequalities, his observation of an inadequate understanding of privacy is supported by public opinion data about the Supreme Court's 2017 ruling that the right to privacy is a fundamental right (see Subsection 6.3.1.1). According to CSDS-Lokniti (2023, p. 219), 84% of survey participants did not know about this judgement. While this indicates a serious lack of awareness of the right, one of my research respondents observed a gradual shift following the COVID-19 pandemic. Arjun claimed that 'slowly people are understanding the importance of data but not really understanding the right to privacy is something given to them'. He attributed this increase to 'tangible harms' like data breaches, and 'intangible harms' like traumatic or psychological impacts SMP users faced online. Despite having different interpretations, both Nikhil and Arjun shared a dissatisfaction about the public's understanding of data and the right to privacy in India.

Second, my respondent Karan deemed awareness to be affected due to the limited transparency in -veillance operations:

I would say the biggest problem with them is that there is no publicly available information about them. So, everything we know about them is pursuant to either right to information requests on statute or investigative journalistic reporting.

By pointing out transparency channels such as ‘information requests’ and ‘investigative journalists’, Karan framed a limited view of how the public can get informed. This observation aligns with failed attempts by civil society organisations to obtain RTI about the use of Pegasus spyware in India (see Subsection 6.1.1.2). The Ministry’s refusal illustrates a deliberative limitation on access to information, directly influencing what the public can know about the use of such -veillance programmes. This limited awareness is reflected in findings from CSDS-Lokniti (2023, p. 158), which show that only 25% of those they surveyed had heard of Pegasus, while the remaining had not heard of it (67%) or didn’t remember (8%). Together, these findings underscore the importance of information for public awareness and its limited availability surrounding -veillance in India.

Overall, the above analysis reflects my respondents’ dissatisfaction with the level of public awareness of -veillance due to inadequate understanding of technology and rights, as well as the government’s limited transparency in India. This highlights how structural factors influence the awareness around -veillance operations and people’s rights and capacity to act within legal frameworks.

6.4.1.2 (Dis)Trust

Democracy

Trust in democracy emerged as a key theme among my respondents. To provide a broader context before my thematic analyses, I first introduce relevant public opinion data before assessing my respondents’ perspectives within the scope of the -veillance theme. According to a 2019 Pew Research Center report, 54% of Indians expressed satisfaction with the way democracy works in the country (Devlin, 2019). Despite this moderate level of democratic satisfaction at state level, my respondents raised -veillance operations and the limitations on individual rights as two critical concerns that reflect distrust in democracy within the context of -veillance.

First, some considered that trust in democracy was being impacted by -veillance. While Ravi viewed surveillance as inherently ‘undemocratic’, Deepa explained that:

Surveillance, especially mass surveillance, hampers the right to privacy and the right to life and liberty, free speech, and it should not happen in a democratic society. In a democratic society a person should have the space to hold their views, their opinions, and those spaces to safely express them without the worry of receiving backlash.

Deepa, a lawyer and legal counsel, reflected on surveillance from an individual rights perspective. She compared how democracies should function in principle with the ‘backlash’ she observed in practice. This aligned with other respondents’ concerns about the right to privacy (Nikhil, Karan). Karan argued that users’ privacy is directly affected by the government’s democratically processed actions, like ‘data requests to individuals and requiring tracing the first originator of a message’. His point illustrates a triadic outcome of the interplay of technology, government, and individuals, whose rights are ultimately affected.

Second, my respondents demonstrated distrust by mentioning restrictions on freedom of speech and self-censorship. Self-censorship entails individuals monitoring and restraining their own speech on social media. One explanation given for this was that ‘everything to be on record’ on social media platforms (Priya). Other respondents shared the view that people are increasingly aware that their posts are visible to others (Deepa, Amit), and this awareness results in self-questioning, as Ravi observed:

Is this something I should say openly? Should I quote my words? Should I try and skirt around the issue? And that’s obviously [...] very concerning because you do want at least a basic level of public discourse to be accessible to any citizen, which is not there now. [...] Because online, I think there are certain things you just can’t say or, if you say, then you deal with the blowback.

Ravi’s questions of ‘Is this something I should say openly?’, ‘Should I quote my words?’, ‘Should I try and skirt around the issue?’ illustrate the internalisation of surveillance, where users self-censor even before posting anything on social

media. The language he used in these questions, such as ‘skirt around the issue’ demonstrates how individuals strategically think and tailor their speech as a result. Like Deepa, Ravi saw the ‘basic level of public discourse to be accessible to any citizens’ as missing, sharing a narrative around the absence of democratic principles in India.

In summary, my respondents viewed the right to privacy as being in conflict with surveillance operations and limiting freedom of speech through self-censorship. They constructed a non-democratic account of -veillance in India, emphasising the gap they observed between what was in practice and the democratic principles that ought to be in place.

The Indian Government

Another theme that emerged from my interviews was a lack of trust in the Indian government, which I first contextualise using public opinion data. In a survey conducted prior to the 2019 elections, the Pew Research Center reported that 64% of Indians viewed politicians as corrupt, while 69% of both BJP and Congress supporters considered their leaders to be corrupt (Devlin, 2019). The same report also showed that public satisfaction with the nation remained slightly above half (55%), though this was a 15% decline compared with the first year of the Modi government in 2017 (Devlin, 2019). Although these datasets refer specifically to the public’s perceptions of politicians, party leaders, and national progress, they collectively illustrate a broader public sentiment of trust and scepticism toward the government. Building on this background, I analyse three thematic concerns reflecting my respondents’ trust and distrust regarding -veillance in the Indian government. These are ID verification, the national security argument, and the implications of -veillance used on the public.

First, drawing on the ID verification requirements, Vikram described ‘India is a low-trust society’. His framing positions verification processes as necessary rather than excessive. In relation to the public, Vikram commented that:

If you support the government, then you trust what they are saying and believe what is being done is done with the best intentions. However, if you are suspicious of the government, you remain suspicious no matter

what they do, even if sometimes they do something right or not necessarily with ill intention.

Vikram used trust in the government as an indicator of one's political position. This assessment was reinforced by Sanjay, who said 'I feel, at least among my friends, including me, we have no trust in the government, we have no trust in the fact that we are not being monitored'. Sanjay further explained:

[...] We have already seen how people tend to avoid going to the police because they are more worried as to how the police will react to them or to their concerns if they were to, say, approach the police. It's the same principle for someone with a lot of power.

Here Sanjay depicted a fearful image of the police and 'someone with a lot of power', constructing a binary of 'us', the people, and 'them', the authorities. This reinforced perceptions of distrust and distance in state-citizen relations in India. These concerns help explain civil organisations' legal challenges against the three surveillance programmes set out in Subsection 6.1.1.2 - the Software Freedom Law Centre (SFLC) and the Centre for Public Interest Litigation's petition to the Delhi High Court regarding CMS, NETRA, and NATGRID in December 2020 (CPIIL and ANR vs. Union of India and Others - Delhi High Court, 2020, as cited in India-FoN, 2021). The Ministry of Home Affairs responded by stating that government agencies do not have 'blanket permission' (PTI, 2021, as cited in India-FoN, 2021), but instead emphasised the necessity of surveillance when dealing with threats (Singh, 2021, as cited in India-FoN, 2021). Such a response not only creates national security arguments but also exemplifies civil society's unsuccessful attempts to get information regarding surveillance operations in India.

Second, my respondents expressed varied views about general distrust in the Indian government due to its use of national security arguments. Arjun remarked that national security and public order were legitimate concerns for any government, as 'they don't want to become Afghanistan'. His reference to 'Afghanistan' illustrates a securitisation narrative, showing how national security arguments are constructed from international examples. This narrative creates a normalisation and justification of such operations, as the public opinion data

show that 52% thought it was acceptable to use CCTV to maintain order in the country (CSDS-Lokniti, 2023, p. 141). In contrast, my respondent Priya criticised the government by saying, 'You [referring to the government] can't hide behind the national security argument forever'. Her phrasing constructed the Indian government as using 'national security' as a justifying mechanism for its actions. Another concern raised regarding national security is the dual-use nature of the tools and operations. As Vikram put it, 'The dual-use analogy is, I think, interesting because it also happens to be a stated reason, right? Security is often a stated reason for a lot of the actions that the government takes'. Like Priya, Vikram's view underscores how security is used by governments to justify dual-use technologies. Together, the language my respondents used demonstrates the prevailing narrative of national security in India.

Third, some respondents approached distrust by discussing the implications that government-linked -veillance operations had for the public. According to a security analyst, Nikhil, state security is prioritised over individuals' security:

[...] the re-identification techniques that are available now to private companies, governments, political parties, security agencies, allow data from social media to be harvested and then be used to create a very comprehensive, like personal psychological profiles of individuals.

Given his expertise, Nikhil highlighted how existing stakeholders can make use of the personal data vested on platforms. His point about 'psychological profiles' indicated individual risks, such as the potential for user manipulation based on the collected data. Regarding the government's dataveillance operations, Arjun noted:

These are misconceptions that the government has, more data access means better control, better tackling of the situations, whereas they're not taking again a balanced approach towards this. Obviously, a certain amount of data you would need, but what is the proportionality of that is something that is not being at this moment done. Also, this is not the Indian case alone, many governments are grappling with how much data is good when it comes to making a better intervention.

The language Arjun used framed the government's data collection as overarching and unbalanced. His emphasis on 'proportionality' positioned the issue from a

democratic lens, while his reference to ‘many governments’ universalised the problem beyond India. In contrast, some respondents expressed distrust arising from allegations of government surveillance, particularly in relation to the Pegasus spyware case. Although the government had neither admitted nor denied its use, my respondents believed this was being used against political opponents (Sanjay, Vikram, Karan). Sharing from personal experiences, Karan explained:

When the Pegasus outbreak happened or the stories were first reported, there was a significant shift to say use Signal instead of WhatsApp. But if you look at the wider population Signal is still very small [...].

Karan’s instinctive turn to alternative platforms such as ‘Signal’ over ‘WhatsApp’ illustrates how government-platform relations vary across SMPs. It also highlights the reflexive monitoring of the agency, showing how these dynamics influence people’s trust and further lead them to self-censor on such platforms. This observation aligns with CSDS-Lokniti’s (2023, p. 156) survey findings, which found that two-thirds of their participants expressed fear of a legal backlash for sharing an online post. One specific case study that emerged from my analysis was Rona Wilson, a human rights activist who was arrested in 2018 (Vincent, 2021 and Hindustan Times, 2021, as cited in India-FoN, 2021). Sanjay mentioned ‘NetWire’ malware and explained:

[...] how the government is using technology and how the government is using its power towards interception to plant fake material onto the devices of the accused in the case. I think his name was Rona Wilson [...] Wilson’s laptop was seized by the police and an examination of the laptop revealed that there were a lot of so-called anti-national content.

To validate Sanjay’s claim, I consulted secondary sources. A report by Arsenal Consulting found evidence that was ‘planted in his computer through a malware’, which led to Wilson’s arrest (Katakam, 2021). This demonstrates not only the misuse of -veillance operations in a targeted way, but also the victimisation of a human rights activist, who was also a journalist in India. Sanjay further commented:

So, the government is not just using its powers to intercept, it's also using its powers to break laws. It is using its power to ensure that it gets a favourable outcome in the country's courts. It is operating as if India is its own fiefdom, that is what we have come down to. It is slowly turning into a banana republic where a certain majority gets to enjoy all the rights provided to Indian citizens under the Constitution, but the minorities, critics of the government, opposition leader, everybody seems to have a target on their back. So, the government interception is being used without any checks and balances. It's happening at a scale which will astonish us, if the government's reports were to actually be made public.

Sanjay framed government interception as unlawful and weaponised, portraying an undemocratic image of the government which is 'break[ing] laws' to secure 'favourable outcomes'. His use of metaphors like 'fiefdom' and 'banana republic' constructed an authoritarian image, where 'minorities', 'critics', and 'opposition' experienced targeted surveillance. This constructs a distrust in the government's use of power, emphasising its politically-biased use and effects.

Overall, my respondents' assessments exposed several problems regarding trust in the Indian government, including polarised politics, the (mis)use of a national security rationale, the use of dual-use technologies, and -veillance operations. Thus, their distrust was affected not only by the functioning of government, but also the way the technology and law were used within the -veillance context in India.

Social Media Platforms

One respondent shared a critical view of his distrust of SMPs within the scope of -veillance in India. Before presenting his thematic insight, I first note existing public perception on -veillance. Public opinion surveys by CSDS-Lokniti (2023, p. 150) show that non-platform users expected higher surveillance intrusion (44%) than those who used them (20%). While this indicates a difference in perceptions between SMP users and non-users, it also reveals a pre-emptive acceptance of surveillance by the former. From a dataveillance perspective, the same report revealed that 70% of survey respondents were concerned about an 'unknown person or company accessing their social media data' (CSDS-Lokniti, 2023, p. 199). This reflects a widespread public distrust toward surveillance and data controls in India.

Acknowledging platforms' dual role in both facilitating surveillance and acting as intermediaries of the government, Nikhil expressed his distrust based on the implications of this for users. According to him, users are treated as 'hostages':

Since social media platforms are one of the kinds of most effective means of communication, still most users are like a hostage because they don't have an alternative. For example, I have my own views on the privacy of, let's say, WhatsApp. I don't really have reason to believe that it's not as secure as they claim it is. But [...] when I live abroad and when I want to talk to my parents, I cannot get them to download Signal or Wire messenger or understand that why it is important to do so. And in that case, I just have to talk on WhatsApp regardless of what my personal views on WhatsApp are.

Here, Nikhil framed dependency on certain platforms as a necessity, regardless of how unsafe they consider those platforms to be. His use of the word 'hostage' demonstrated his sense of desperation and lack of similar alternatives, since platforms like 'WhatsApp' have become core channels of communication. This shows how SMPs are integrated into society, influencing personal communication practices, leaving individuals in a desperate position.

6.4.2 United Kingdom

6.4.2.1 Awareness

In line with the definition given in Subsection 6.4.1.1, this subsection investigates my respondents' observations on the public's understanding of two critical aspects of -veillance. These are the common understanding of -veillance operations and their normalisation in the UK.

First, some respondents approached awareness by explaining the common understanding of -veillance issues. From a data collection perspective, Sarah asserted:

It strikes me that people's appetite to embrace technology [...] so these are voluntary decisions that people are making, such as Alexa [...] research studies have routinely gathered during COVID, because people have this desire to act in the public good. So, they share all sorts of personal data they didn't normally have.

Sarah's emphasis on 'COVID' and people sharing data 'they didn't normally have' illustrates how moments of crisis can render data collection voluntarily. This aligns with the Centre for Data Ethics and Innovation's (2022, p.19) survey showing that 19% of people believed their data could improve responses to COVID-19 and benefit the public. Despite these widely held views, Jessica highlighted the increasing care taken after the Snowden revelations, by 'usually the people who are at the forefront, right, like lawyers, journalists, activists, who are fighting for that and who have a bit more awareness'. She described awareness of -veillance as unevenly distributed, where certain sectors that were 'at the forefront' had more understanding. Similarly, Richard argued that the 'public by and large don't understand how this is undermining their democracy [...] I think we've become very normalised to the level of surveillance that we have in the UK'. Richard's emphasis on democracy being 'undermined' highlights a critical narrative about the common lack of awareness about surveillance's implications and its normalisation in the UK. Such normalisation creates a concern about the form of digital governance, leading to the next point.

Second, respondents observed the normalisation of -veillance practices in the UK, especially during of crises. Sarah asserted that 'there are times where proportionate and reasonable and lawful interference can take place, and a public health emergency is one of them [...] COVID has been the game changer'. The language Sarah used illustrates a securitisation narrative, where certain emergencies, like 'COVID', justify 'lawful interference'. From a different perspective, Jessica criticised the case, annoyed that 'data collection is presented as the only solution'. This criticism questions the practical usefulness of data collection through a security discourse, as another respondent, Richard, argued that 'we're not really presented with coherent data that would show us that surveillance is making us safer'. Together, these respondents' insights suggested that the public was getting acclimated to the idea of -veillance, even when there was little or no evidence to determine its effectiveness or confirm whether violating individual rights was essential for promoting security.

Overall, my respondents constructed an image of normalisation and uneven unawareness of -veillance operations in the UK. This underscores the relevance

of professional and lived experience in shaping public understanding of -veillance operations and democratic principles.

6.4.2.2 (Dis)Trust

Democracy

(Dis)Trust in democracy was one of the patterns that emerged from my interviews. Before analysing their insights, I first contextualise the issue in the country through public opinion data. Based on the Electoral Commission's (2023) 'Public Opinion Tracker', only 33% people were satisfied with the way democracy works in the UK. My analysis identified three respondents who gave different views about trust in democracy regarding -veillance. Richard argued that -veillance operations affect the 'basic tenets of a democratic society', clashing with democratic principles in practice:

I think everybody wants to point the finger at countries like China [...] they're trying to protect anything that would undermine the state. Okay, so we might not like the state and its rather undemocratic principles, but in one sense that's no different to a UK government saying, 'we need to do this because we need to protect democracy'. Really? How do you protect democracy? By spying on your population or overregulating your population? [...] So, the Chinese do what they do pretty overtly to protect their ideology, most Western governments do what they do covertly and claim that they don't do it to protect their ideology, but what they're actually ending up doing is undermining their ideology, if that ideology is democracy. And I think, unfortunately, much of what Western governments do tends to be tied up and justified under the umbrella of counterterrorism, however you want to define that.

Richard's comparison of Western democracies with China underscores the contradictory narrative in which opposing regimes engage in similar practices. By contrasting China's 'overt' practices with the UK's 'covert' ones, he depicted China as a more transparent and accountable regime than the UK, which 'undermine[s] their ideology'. In doing so, he questioned the democratic credibility of democracies themselves and constructed a securitisation narrative in which they justify -veillance under 'counterterrorism'. Unlike Richard, Lauren considered excessive monitoring as:

This is a form of digital authoritarianism perhaps in a more conventional sense of what China is doing right now [...] it's not like that of course because liberal democracies do this in very, very different ways and it's always the case that censorship is done in a less formal way and less transparent way, but I feel that state governments are moving into that more and more and that we can absolutely expect that there are interferences [referring to government interference] with social media platforms to increase [like digital authoritarianism] rather than going the other direction [unlike the democratic side].

Lauren's view presented a less critical comparison between democracies and authoritarianism than Richard's. While she acknowledged a shifting 'direction' in democracies, her emphasis on 'liberal' democracies being different from China illustrated how such transformations occur in subtle and silent forms. In contrast to both Richard and Lauren, Jessica did not perceive democracy as having an end:

Democracy is something that you need to keep on fighting for [...] a lot of the time there's a perception of totalitarian regimes being kind of spying all the time, but the same mechanisms are happening in more democratic countries, they're just portrayed in a different way.

Jessica's view of democracies as 'something that you need to keep on fighting for' constructs it as an idealistic form of governance that requires continuous effort. Like Richard, she highlighted how narratives are shaped differently across regimes, despite similar practices.

Overall, all three of my respondents expressed their views by comparing democracies with authoritarianism. My analysis shows how they constructed an image of a democratic transformation towards authoritarianism in the digital sphere. This finding highlights not only a shared view that democracy was weakening online but also provides primary insights into digital governance from the UK context.

The UK Government

Distrust in the UK government emerged as another pattern from my interview data analysis, showing an alignment with public opinion data. According to the Office for National Statistics (ONS, 2024), 57% of people reported having either

low or no trust in the government in 2023. Acknowledging this limited level of public trust in general, I analyse three concerns raised by my respondents regarding trust in the UK government's handling of -veillance. These are the government's stance on privacy and encryption, data collection practices, and their influence on individuals.

The first concern emerged regarding the government's criticism of privacy and opposition to encryption, which specifically led to personal security issues.

Focusing on encryption, Mark remarked that:

When a new Home Secretary takes on the position, usually within three weeks they have issued some statements about 'We must fix end-to-end encryption' [...] And they're going to use emotive examples such as child abuse images. Even though what they want to do is a massive blanket of measures that will affect all sorts of things [...].

Mark's observation illustrated a securitisation narrative, where Home Secretaries present 'encryption' as a 'child abuse' threat, justifying expansive measures that will affect other areas. His observation complements the Five Eyes collaboration mentioned in Subsection 6.1.2.2. Another respondent, Tom, approached the government's interest in breaking encryption from an individual security perspective, arguing that 'decrypted conversations will not be only visible to the government but also criminals, and put us at risk'. His point raised the dilemma of state security versus personal security. Both respondents expressed distrust towards the government as stemming from its institutional power to manage encryption.

The second concern raised by my respondents related to the government's data collection practices. Richard approached this by discussing the government's intention to obtain the same amount of data held by SMPs, which he described as 'extremely dangerous':

Governments simply want that exact same information. And generally speaking, democratic governments, they can't access it directly from the social media companies [...]. So, what happens quite a bit in the UK I understand is that there is a lot of surveillance that takes place where police forces and other agencies will collect data and carry out profiling,

maybe even using facial recognition technology for surveillance as well, to try and build more information about individuals.

Richard framed government surveillance operations as a strategic effort to gather and process SMP data, underscoring the competitive and multi-stakeholder environment of the digital sphere. Similarly, Jessica argued that:

Data collection is a very problematic tool that is often abused by governments [...]. We need data collection of a shooter, that is fine; but when the government is stating suspicion and collecting that person's data as well as the close friends' data, this should be limited.

Here Jessica gave a critical narrative of government data collection, asserting that only certain individuals' data are necessary for security, not everyone's. From a personal security perspective, Tom argued that the data used to verify age is confidential and criticised the collection of 'passport, credit cards, or other IDs'. His concern highlighted potential outcomes of the government's age verification plans, creating additional risks for individuals. Collectively, my respondents' reflections aligned with public opinion data showing that only 47% of UK adults trusted the government to use their data legitimately (ONS, 2024). Together, these insights illustrate a broader scepticism around the government's collection and use of data responsibly in the UK.

The third concern they raised related to the government's justification for using technologies that infringe individual rights. According to Jessica:

I think it's quite similar actually to totalitarian regimes. It's always about the protection of the population and 'we're concerned about you, and we want to keep your rights'. And then at the same time [...] if you are a law-abiding citizen then you don't have anything to hide, and this should all be fine. So, it's this kind of dual effect and trying to present that it's for the protection of people.

Jessica's point highlighted the dual implications and normalisation of infringing individual rights by generating guilt, which, in turn, leads to self-censorship. Based on personal experience, Emily explained that self-censorship can lead one to take preventative measures to avoid tracking, such as 'using VPN when accessing a political party's website' or 'hiding when checking someone's profile

on LinkedIn'. Although these were her own methods of practicing self-censorship, they illustrated her perspective as a researcher when engaging with political or sensitive content online.

In summary, the analysis of my respondents' concerns about the government's stance on privacy and encryption, data collection practices, and their influence on individuals highlighted their discomfort with the government's -veillance management in the UK. Their views point out a strong securitisation narrative in how -veillance is practiced by authorities, influencing data collection and individuals' self-censorship.

Social Media Platforms

My respondents raised trust in SMPs as a contested issue in the UK. Before analysing their insights from a -veillance perspective, I incorporate relevant public opinion data to situate their views within a broader context. According to the Office for National Statistics (ONS, 2024), 8% of UK adults considered social media a key issue in the country. While this highlights public recognition of SMPs as one of the national concerns, I expand on this by analysing Mark and Jessica's views on distrust in SMPs in relation to -veillance.

Mark shared his distrust of SMPs based on the power they have acquired, stating that 'the richest 100 people are constantly getting richer, while the rest of us are not'. He compared the power held by the government and SMPs:

I've been moaning about governments forever, but maybe at least the government, in theory, is supposed to be answerable to you and to me; Elon's not answerable to either of us. [...] So, you could argue that, if I've got to have surveillance by a country and a government or surveillance by a billionaire lunatic, and I think I might rather pick the government as the least worst option.

Although critical of both stakeholders' surveillance operations, Mark's comparison constructed SMPs as more problematic than the government, citing issues of public accountability. Unlike the more systematic governance of states, his example of 'Elon' [Musk] illustrated how immense power can be concentrated in a single individual.

Jessica expressed her distrust in SMPs through self-censorship. Drawing on her research experience and personal choices, she explained:

What we have shown in our project [...] actually that the majority of the people don't post online. So, what happens is that you have a small minority that is posting online and then people can share it or consume it in different kinds of ways. [...] On the other hand, because a lot of the stuff that is online is not going to be deleted and it can be used against you in multiple ways, then you censor yourself. I find that myself in the past decades or more I've used social media, because I know that my political views or any kind of views can be used against me.

Here Jessica not only underscored the characteristics of the digital sphere, like not having control over what is published, but also indicated that online engagements are limited to certain people. Similar to Emily's personal example in the previous subsection, Jessica framed self-censorship as a preventive strategy that helps users feel secure when engaging in digital activities. Additionally, her point on the long-term consequences of sharing political views reflects a widespread concern of the public. According to Election Commission (2023) data, 56% considered political activities on SMPs to be inadequately regulated (Electoral Commission, 2023). Thus, such unregulated spaces leave people to reflexively find solutions, like self-censorship.

While Mark expressed his distrust through a structural level by comparing governments and SMPs, Jessica's view reflected an agency-level reaction to the existing -veillance ecology on platforms. In sum, this section analysed my respondents' views and the language they use about trusting -veillance in the UK. Their contributions brought together different perspectives that explained -veillance through democracy, government, and SMPs.

6.5 Conclusion

-Veillance was the first theme generated by my analysis of the digital governance of SMPs in India and the UK. Following my examination of surveillance and dataveillance in both countries, this chapter can be summarised in six points.

First, the identified operations contextualised how both countries integrated -veillance into their digital governance. Government-linked operations employed both technical and non-technical methods, reflecting India and the UK's structural adaptations and use of technology. Government collaborations stressed the multi-stakeholder environment of the digital sphere, highlighting the actors involved in operations. Together, these operations demonstrated the interplay between governments, actors, rules, and their operational practices. This not only revealed the socio-political landscape of -veillance in both countries but also offered insights into how technology was interpreted by different actors and structurally integrated within their contexts, thereby contributing to the construction of digital governance.

Second, my analysis of SMPs' transparency reports revealed that both governments requested more data from Facebook than from Twitter. Between 2019 and 2021, India made 220,899 requests to obtain data on 342,993 Facebook accounts, while the UK made 56,605 requests regarding 68,736 accounts. Various factors may explain this disparity, such as digital demographic differences (see Subsection 3.1) or the relationship between these SMPs and governments, as highlighted by my respondents. Taken together, these analyses illustrated both platforms' structural - the platform procedures they followed in providing data to governments - and agency dynamics, like the reflexivity and capacity to act contrary to government requests. Acknowledging different findings on both countries, this analysis not only revealed contextual differences about the role of SMPs but also reflected further on the multi-stakeholder environment of digital governance by specifically focusing on the two SMPs.

Third, respondents from both countries expressed concerns about government-SMP relationships. They mentioned SMPs' power over data and governments' reliance on platforms to access such data. These two common concerns emerged in both countries, illustrating an interdependent relation between SMPs and governments. Specifically, my Indian respondents pointed out the lack of detail in SMP reports and suggested a need for a shared government portal. This assessment addressed the diversity of players within data collection and the complexity this creates in following these exchanges on digital governance. In

contrast, the UK respondents suggested that SMPs' data collection was a form of service payment made by users. Together, these country-specific perspectives reflected my respondents' interpretations of -veillance shaped by national contexts, offering primary insights into the role of SMPs.

Fourth, both democracies enshrine people's rights to privacy and to request information in their legal systems. Considering my normative framework based on liberal internationalism, this reveals both democracies' consideration and integration of the universal principles into their state legislation, which encompasses the digital sphere as well. However, my review also shows that both these rights are limited in India and the UK, meaning that the preservation of people's rights and their capacity to act as agencies could be restricted by the structure created under the law. This limitation reinforces my methodological choice to include and review the legislation relevant to -veillance in both countries, as the next point summarises.

Fifth, both countries had several pieces of legislation regarding permitting and regulating -veillance. I found that the existing frameworks included the implementation and interpretation of legislation enacted before the World Wide Web, like India's Telegraph Act of 1885, and those developed after its emergence, like the IT Act (2000) in India and RIPA (2000) in the UK. These legislative changes underscored both countries' adaptation to the emerging technologies and construction of their law to control not only the technological aspects of -veillance or SMPs but also the legal conditions under which agency operates. These shifts about the creation, implementation, and protection of rights did not eliminate legal concerns in both countries. My respondents from India raised concerns about the making of the Bill and criticising the laws being state-centric, while UK respondents highlighted multiple interpretations of the law and raised data management concerns. Together, these illustrate the national dynamics of how law structurally interacts with -veillance in both countries, reflected on with the primary views of the people I interviewed in my research.

Finally, my respondents from both countries shared similar assessments of -veillance within their countries. Despite different explanations and reasonings, they raised the issues of awareness and (dis)trust in democracy, the government, and SMPs as core observed implications of -veillance on the public. Together, these assessments responded to and reflected views on digital dual-use operations, the role of SMPs, and the legal frameworks findings presented earlier in this chapter. Their comments also considered the forms of digital governance practiced in each country, highlighting democratic and authoritarian debates.

This summarises my findings on -veillance in India and the UK. The empirical evidence presented on the socio-political context of -veillance operations, the role of SMPs, legal frameworks, and the observed implications on sections of the public offer significant insights about digital governance and its structuration. With different primacies described across my analysis, the four parts of this chapter have collectively foregrounded the contextual interplay of structure, agency, and technology in relation to my empirical findings on -veillance. In doing so, this chapter thematically contributes to the overall discussion of digital governance of SMPs in India and the UK, given in Chapter 9. The next chapter introduces the second theme of my research.

Chapter 7 Content Control in India and the UK

Content control is the second theme generated by my research to explore the digital governance of SMPs in India and the UK. This chapter presents my research findings in four parts.

Part 7.1 presents identified operations regarding content control within the socio-political contexts of India and the UK. These are primarily drawn from my thematic analysis of the FoN reports and integrated with interviews and data source triangulation for a more comprehensive assessment. This analysis explores how content control technologies were practiced by different actors and integrated within state structures as part of the digital environments of the two countries.

Part 7.2 examines SMPs' role in content control. It analyses 'Content Restrictions' reports from Facebook⁶⁷ and 'Removal Requests' reports from Twitter⁶⁸ between 2019 and 2021. Unlike in Chapter 6, I analyse these reports separately, as the platforms' structures for processing such requests differ. This is followed by my respondents' assessments of SMPs and, when relevant, with FoN reports. Together, these analyses conceptualise SMPs as both structures and agents, defined by their interactions with governments and technological dynamics.

Part 7.3 reviews existing legal frameworks by analysing individual rights, state legislation⁶⁹, and legal concerns related to content control. It draws on FoN findings, supplemented with deliberative secondary data review and qualitative interviews. Building on my liberal internationalism framework, I incorporated Article 18, freedom of thought, and Article 19, freedom of expression, of the Universal Declaration of Human Rights (1948)⁷⁰ into my consideration. This analysis aims to understand the constructed legal structure within the scope of

⁶⁷ See Appendix 9 for full data on India-Facebook; see Appendix 11 for full data on UK-Facebook.

⁶⁸ See Appendix 10 for full data on India-Twitter; see Appendix 12 for full data on UK-Twitter.

⁶⁹ See Appendix 4 for legal extracts and notes on analysed individual rights and state legislation in both countries.

⁷⁰ See Appendix 4 for legal extracts and notes on the Universal Declaration of Human Rights.

this theme and explain how it engages with technology and agency in both countries.

Part 7.4 explores the key concerns and implications raised by my respondents and FoN reports regarding the public in the two countries. To validate these agency-level insights, I employed data source triangulation incorporating other relevant secondary sources. Both parts present India and the UK in separate sections. Before presenting my research findings, I define content control within the scope of this thesis.

As illustrated in Table 7.1, content control is made up of two sub-themes: content blocks and content removals. Content blocks refer to restricting access to certain materials, while content removal involves taking down materials, including manual and automated removals, among other methods listed in Table 7.1. While these two sub-themes have some variances, there are instances where they become interconnected. Finding this interlinkage led me to merge them into a broader theme, which I have called content control. I define content control as the blocking and removing of content in ways including, but not limited to, those listed in the table. I characterise it as a dual-use concept, meaning that content control can be used in both beneficial and harmful ways (see Chapter 1 for a brief literature review on dual-use).

Table 7.1: Content Control	
Content Blocks	Content block, content filter, blocked website/URL, banned application, blocked domain, optional filters, parental filters, child filters, over blocking, censorship.
Content Removals	Content moderation, content takedown, content restriction, forced content removal, removal of online material, content removal, automated content removal, child filters.

7.1 The Socio-Political Landscape of Content Control Operations

7.1.1 India

My thematic analysis of the FoN data showed that India blocks content on topics including: ‘anti-Indian sentiments, pornography, pirated content, and content that could damage public order, the security of the state, and the interest and defence of India’s sovereignty and integrity’ (India-FoN, 2019-2021).

Additionally, content removal includes: ‘pornographic content, social and political content containing hate speech, anti-religious (Hindu), violence, extremism, anti-state, defamation, privacy, security, criminal acts, disinformation and misinformation, COVID-19, critiques to the current government and the Prime Minister, and illegal content that risks public safety and security’ (India-FoN, 2019-21). These lists demonstrate the extensive topics deemed suitable for content control in India. To examine how this was operationalised in the country, I present my FoN findings based on the two categories of operations described by my respondents: direct and indirect ways.

First, a public policy professional, Tarun, described the ‘direct way’ as the government removing content under the law. I combined this with formal and regulatory mechanisms that I gathered from FoN, such as the Department of Telecommunications (DOT), government orders, court orders, orders from the Election Commission at election times, and the law⁷¹ (India-FoN, 2019-21). One specific example of direct operations is the Cyber Crime Volunteers Programme, which was introduced in my -veillance theme (Subsection 6.1.1.1). This allows citizens to voluntarily assist law enforcement. The literature I identified from the FoN reports notes that this programme offers several positions⁷², including an unlawful content flagger (The Economic Times, 2021). My respondents’ opinions on this programme differed. Tarun shared an optimistic view of the programme:

Trust flagger programmes are actually more for child sexual abuse materials, extremist content like that [...] because you [referring to

⁷¹ See Section 7.3.1.

⁷² ‘Cyber Volunteer Unlawful Content Flagger, Cyber Awareness Promoter, and Cyber Expert’.

volunteers] have some expertise [...] I think the trust flagger programmes are definitely good. And, as far as I'm aware, [...] platforms usually don't have the ability to report the kind of content we are talking about.

Tarun's emphasis on the platforms' 'ability' framed SMPs as inadequate regulators, reinforcing the need for such a programme. Unlike Tarun, Vikram commented that:

A lot of people don't necessarily know about it, people like me who follow it [referring to the programme], we have little information [...] It's not at that scale, but I think if it were to get to that level of awareness it certainly has had the potential to do that because you're essentially incentivising citizens to surveil each other, to spy on each other, and then complain or report them to the police [...] they're [referring to the volunteers] likely to be out there scanning for content and reporting 'problematic' content [...]. Who considers what problematic is based on the interpretation of that volunteer and of the police, whether they want to pursue it [...] it's a certainly concerning programme, it had the potential to be divisive, but awareness is not at that scale where it's actively preying on a lot of people's minds.

Vikram's take on the programme as 'incentivising citizens' framed it as promoting surveillance within the public. He highlighted individuals' 'interpretation' and general 'awareness' as problematic outcomes of such a programme for society. Despite its unpopularity with the public at large, this decentralised operation comprises a direct government programme in India.

Second, indirect government operations include 'criminal sanctions imposed' on SMP representatives to ensure their content control compliance under Indian law (Karan). My FoN analysis identified two examples: technical filtering operations and Netsweeper. Technical filtering operations involved external content control tools used by the government. Studies cited by FoN found that two service providers, Airtel and Jio, employed 'Server Name Indication (SNI)-based filtering', which allow the monitoring of users' unencrypted online activities and 'restrict access based on government orders' (Open Observatory of Network Interference, 2020; Ahmed, 2020; and Agrawal, 2020, as cited in India-FoN, 2021). This demonstrates state collaboration with service providers in defining the use of technology in India.

Netsweeper, an internet filtering tool developed by a Canadian company, was found to be deployed at the national level in India (The Citizen Lab, 2018, as cited in India-FoN, 2019-2021). According to the Citizen Lab's report, Netsweeper blocked 1,158 unique URLs and removed political posts, including those addressing 'Rohingya refugee issues and deaths of Muslims in Burma and India' from platforms such as Twitter, YouTube, and Facebook (Dalek *et al.*, 2018, p. 55). While these posts were only accessible in HTTP format, the use of Netsweeper revealed the external deployment of a dual-use tool and government censorship targeting religion in India. This illustrates the influence of state-level issues on digital content control operations (see Chapter 3).

Overall, my analysis reveals direct operations as those involving not only the central government and legal mechanisms but also a lateral programme that decentralised these operations. In contrast, indirect operations refer to actors in relation to content control operations beyond the government and relied on external tools and filtering systems within India's digital structures. Despite their variations, this account of these operations contextualises the multi-stakeholder nature of India's digital governance and illustrates how technology is integrated within them.

7.1.2 United Kingdom

My analysis of FoN data found that the UK primarily controls content in three categories: copyright infringement, promotion of terrorism, and depictions of child sexual abuse (UK-FoN, 2019-2021). Following this brief overview, this section reviews four forms of content control operations in the UK: the Internet Watch Foundation, service providers, government departments, and under the law.

The first form of content control involves operations through the Internet Watch Foundation (IWF). IWF is an independent body that works with other organisations on issues related to child sexual abuse content (Internet Watch Foundation, n.d.). While earlier reports noted that it was initially funded by the European Union and industry bodies (UK-FoN, 2016), the Internet Watch Foundation (n.d.) remained based in the UK after Brexit and is now supported by

‘private donors and member companies’ from relevant sectors. It operationalises content control by compiling lists of URLs reported by citizens and hotlines, then sharing them with the site owners - including ISPs and SMPs - to block the content (Internet Watch Foundation, n.d.). However, given the nature of content blocks, there is a lack of transparency around knowing which sites have been blocked for hosting child sexual abuse, as the list is not public (UK-FoN, 2019). Mark, who is a retiree from the IT sector and author, perceived IWF’s role against child abuse as promoting justice: ‘they were set up [...] to try to find the victims and try to prosecute people who have created and distributed these images’. Based on his experience, Mark underscored IWF’s technical support for the companies, stating that ‘[company name] paid them a few thousand pounds a year [...] and all the other ISPs pay for this service as well’. His insights not only confirm the IWF’s role in operations but also highlight it as a medium in the interplay of service providers, government regulations, and digital content.

The second form consists of service providers’ operations, which vary between ISPs (internet service providers) and MSPs (mobile service providers). ISPs block URLs according to the Internet Service Providers Association’s Voluntary Code of Practice, while MSPs block content by paying for IWF’s service, as detailed above (UK-FoN, 2016-2021). Although FoN reports from 2016 to 2021 described this as a form of legal content filtering, differences between ISP and MSP filtering mechanisms create disparities in access to legal content. For instance, the British National Party’s website was rendered inaccessible for O2 customers only (Brewster, 2012, as cited in UK-FoN, 2019-21). Another example was a dating site that was blocked on all ISPs except Virgin Media (Mackenzie, 2014, as cited in UK-FoN, 2019-21). While these examples highlight disparities among customers of different service providers, the ‘Blocked!’ project of the Open Rights Group, a London-based non-profit organisation, showed that websites were mistakenly blocked by service providers as a result of using child filters (Blocked!, n.d., as cited in UK-FoN, 2021). It found that service providers have inadvertently blocked websites including schools, LGBT+ groups, counselling bodies, charities, and religious organisations, among others (Blocked!, n.d., as cited in UK-FoN, 2021). These examples illustrate the service providers’ diverse

content control operations and the impact this has on their customers, leading to problems of inconsistent blocking of legal content or over-censorship.

Furthermore, ISPs have the power to employ automated blocking and filtering tools, if they fit into their terms and conditions under the law (Section 104 of the Digital Economy Act, 2017, as cited in UK-FoN, 2019). One example of this was BT building a filtering technology called Cleanfeed in 2004 to block child sexual abuse content (Bright, 2004 and Arthur, 2008, as cited in UK-FoN, 2019-21). My respondent Anna described Cleanfeed as ‘the first mass censorship of the web attempted in a Western democracy’. Despite democratic concerns, the UK High Court ruled that BT could employ Cleanfeed on Newzbin2, a website where copyrighted materials were accessible illegally (20C Fox v BT, 2011; UK-FoN, 2019-21). Similarly, the Terrorism Act 2006 allows ISPs to use child filters on content in order to ‘prohibit[s] the glorification or promotion of terrorism’ (Wintour, 2014, as cited in UK-FoN, 2016-21). These examples highlight how ISPs’ filtering systems developed to control child sexual abuse have been expanded to include copyright and terror issues under the UK’s judicial system. They also exemplify the integration of three categories of content control in one operational practice.

The third form of operation is those that are conducted by the government departments. For instance, under the Terrorism Act 2006, the Counter Terrorism Internet Referral Unit (CTIRU) removes content that ‘glorifies or praises terrorism, could be useful to terrorists, or incites people to carry out or support terrorism’ (Open Net Initiative, 2010, Terrorism Act, 2006, and National Police Chief Council, as cited in UK-FoN, 2016-21). These operations are implemented through takedown orders issued by police to intermediaries, illustrating a form of duality between the two.

Another example is the development of automated tools for content control in collaboration with the Home Office. My analysis shows that the need for such technology was socially constructed. Ben Wallace, a former Conservative Party Security Minister (2016-2019), criticised SMPs and other companies for their slow response in dealing with radical content and argued that this delay was ‘forcing

government to act instead’ (Vardy, 2017; Vardy, 2017, as cited in UK-FoN, 2021). One such development emerged from the Home Office’s collaboration with ASI Data Science, for producing a tool that automatically detects online content containing the terms ‘IS’ or ‘Daesh’ (Greenfield, 2018, as cited in UK-FoN, 2021). This reflects the UK’s response to the observed gap on SMP governance, as criticised by Ben Wallace, and illustrates the development of dual-use technologies within its digital governance framework.

Finally, the fourth form of operation is conducted under the law. While Subsection 7.2.2.1 outlines a descriptive analysis of the content removed from platforms, Subsection 7.3.2.3 addresses the legal frameworks surrounding this operation in the UK.

Overall, these four forms of operations illustrate both the central and de-centralised approach the UK has to its content control. Considering the role of the IWF, ISPs and MSPs, as well as the CTIRU and the law, this analysis highlights the diversity and multi-stakeholder nature of the UK’s digital governance, and how these different actors have adapted technology in relation to content control.

7.2 The Role of Social Media Platforms on Content Control

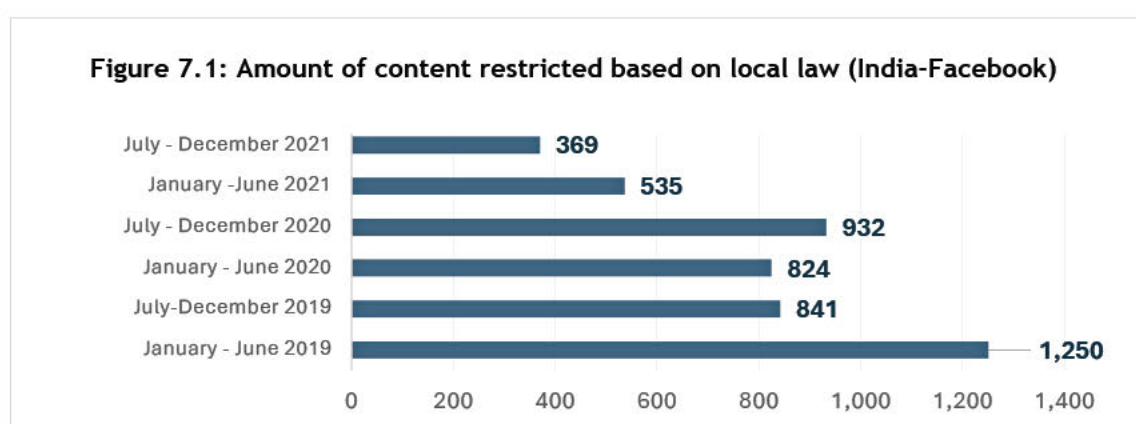
7.2.1 India

7.2.1.1 Transparency Reports

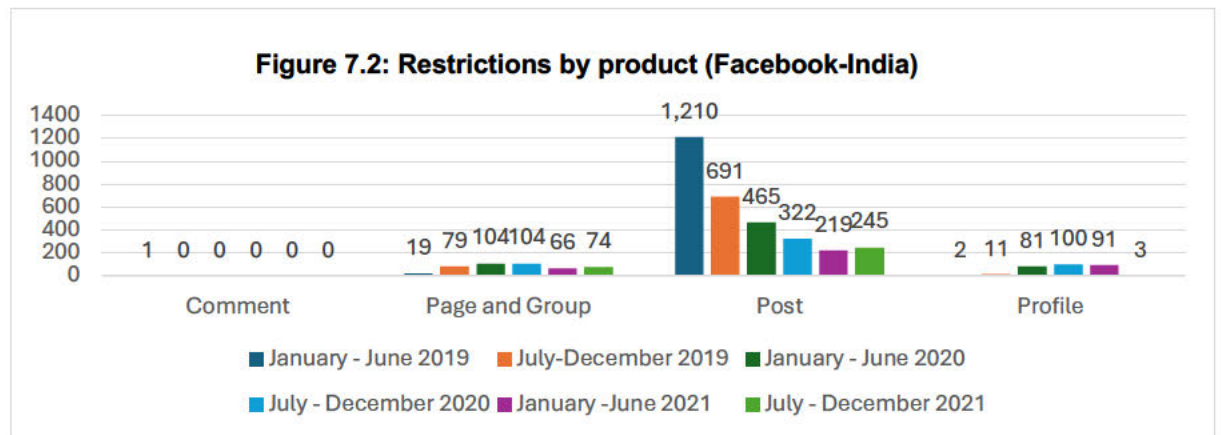
This subsection first analyses content restrictions from Facebook under the law and then the removals requested from Twitter in the context of India. By doing so, it examines each SMP separately to examine their platform structures surrounding content removals and their capacity to respond to government requests.

My analysis focuses on two aspects of content removal from Facebook: the total number of content pieces restricted and the restrictions by product in the country. First, as Figure 7.1 shows, the total number of contents restricted in

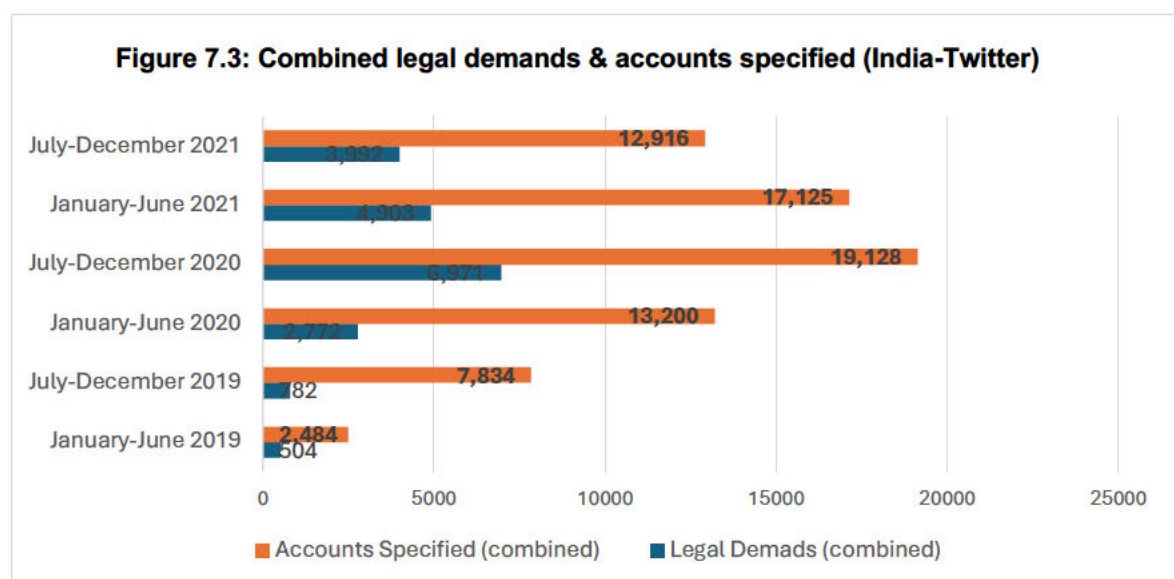
India was 4,751 between 2019 and 2021. During these three years, the lowest number of content restrictions on Facebook was 362 in July-December 2021, and the highest number was 1,250 during January-June 2019. Overall, an average of 791.3 pieces of content were restricted on Facebook every six-months, showing how the law is used for content removals on the SMP. Unlike the observed increase in government user data requests in July-December 2021 (see Sections 6.4.1 and 6.3.1), content restriction can be seen to have declined between 2019 and 2021.



The second aspect is the content types, called ‘products’ by the platform, that were subject to restrictions on Facebook in India. As set out in Figure 7.2, each product is accompanied by six figures from the platform’s biannual reports between 2019 and 2021. This shows that the most restricted product was Facebook posts - 3,152. The second most restricted product was pages and groups, which Facebook restricted 446 of during the selected three years. The third highest restricted product was user profiles - 288 - and the least restricted product was a single comment. These numbers objectively rank content control products under the law, shedding light on specific areas where user engagement was affected by Facebook’s content control operations in India.



Following Facebook, I analyse Twitter's content removal by focusing on two key areas: the combined number of legal demands received from India and the platform's compliance rate. First, Figure 7.3 portrays the total number of legal demands and accounts specified in India. It shows that Twitter received 19,924 requests for 72,687 accounts between 2019 and 2021. Unlike Facebook, Twitter received the lowest number of legal demands (504) and accounts (2,484) between January-June 2019. In contrast, July-December 2020 was the period of the highest legal demands (6,971) and accounts specified (19,128) received by Twitter. These numbers mean that Twitter received an average of 3,320 demands to remove 12,114.5 accounts every six months. Although Twitter received 15 times more demands than Facebook, it did not comply with them all due to its unique platform structure, which I analyse next.



Unlike Facebook, Twitter processed legal demands within its platform structure. Table 7.2 illustrates the number of accounts specified in these legal demands and the percentage compliance rates. It is important to point out that the platform did not start reporting this until July-December 2019, therefore, the first biannual compliance rate is not shown. By applying compliance percentages to the accounts specified, I ascertained the total number of items removed by Twitter in India during those two and a half years, 10,989⁷³. These numbers show that Twitter's lowest compliance was 1,740.6 accounts during July-December 2020, while the highest was 2,975 during July-December 2019. This means that Twitter only complied with 10,989 out of 72,687 account requests, which makes an average rate of 18.2% compliance.

Table 7.2: Compliance rate of Twitter-India						
India-Twitter (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July-Dec 2021
Accounts Specified (combined)	2,484	7,834	13,200	19,128	17,125	12,916
Compliance rate	N/A	36.7%	13.9%	9.1%	11.8%	19.5%
Number of accounts removed	N/A	2,875.078	1,834.8	1,740.648	2,020.75	2,518.62

Given the different approaches of Facebook and Twitter, this subsection concludes with a brief comparison of the two platforms. Unlike the government's user data collection method outlined in Subsection 6.2.1.1, Facebook had a lower number of content removals, 4,751, than Twitter, 10,989 in India. Thus, although Twitter did not fully comply with government requests, as Facebook did under local law, it still removed more content. When their

⁷³ Full number: '10,989.896'.

platform structures are compared, Twitter illustrates its capacity to act otherwise to legal demands by relying on its internal procedural mechanism, whereas Facebook's structure acts in accordance with local law, demonstrating the power of law over its platform operations. To further evaluate SMPs role in the context of India, the next section presents my respondents' views on SMPs' role in content control.

7.2.1.2 Assessing the Role of SMPs on Content Control

This subsection analyses my respondents' assessments of SMPs and supports this qualitative data with FoN reports where relevant. The analysis is structured around two points: the government's relationship with both platforms and SMPs' business nature regarding content management.

First, my respondents' assessments of the relationship between the Indian government and Facebook and Twitter contained distinct evaluations for each platform. Some highlighted Facebook's exclusive relationship by pointing out its pro- or anti-BJP content removal decisions (Ravi, Vikram). This can be supported with an example from FoN reports, which detailed Facebook's blocking of the '#ResignModi' hashtag several times, 'but claimed that the move was done accidentally' (Deep *et al.* 2021 and The Hindu, 2021, as cited in India-FoN, 2021). Ravi described Facebook's position in India as: 'Facebook is massive red. They obviously want to stay in India. If they want to stay in India, they have to adopt a certain friendly face towards the government'. Ravi framed Facebook's dependency in India as contingent on adopting a 'friendly face towards the government', emphasising on the platform's strategic collaboration with the country.

Unlike Facebook, some respondents perceived Twitter as having an antagonistic relationship with the Indian government (Priya, Amit). This aligns with FoN reports which show that Twitter initially complied with the government's blocking requests but later restored those posts to protect freedom of speech during the farmers' protests (Hindustan Times, 2021, Financial Express, 2021, and Bhargava, 2021, as cited in India-FoN, 2021). In return, the Indian government warned Twitter about Section 69A.3 of the IT Act, reminding them

that noncompliance with its orders could result in a financial penalty or up to seven years of imprisonment (Singh, 2021 and Doval, 2021, as cited in India-FoN, 2021). Following the 2021 IT Rules, Twitter sued the Indian government at the Karnataka High Court for its mass content removal requests and infringing individual rights (Vikram; Singh and Conger, 2022). These examples highlight the Indian government's collaborative relationship with Facebook, while indicate a more confrontational one with Twitter.

Second, despite Facebook and Twitter's differing relationships with the government, my respondents stressed their business operations in India. Ravi pointed out the important role Indian users play in the SMP market: 'India is such a big market for all these companies'. This is true not only because of India's large digital population (see Section 3.1 for demographic details), but also its geopolitical effect, as explained by Nikhil:

If we look at the latest reports in terms of the growing audience members of social media platforms, we can see the major platforms, for example, Facebook or Instagram, which are part of Meta, are seeing steady decline in the number of new users. And this is because the user base within the Global North let's say has been saturated. And therefore, the only new users left to be brought online are those who have not yet been granted access to the internet living in the Global South, where the spread of economic and social and educational opportunities are not as widely spread. And therefore, there's a growing incentive for social media platforms to have to work hand in glove with governments that are often liberal democracies, or worse, authoritarian or repressive regimes, in order to ensure their own survival as well.

Nikhil's comparison of the Global North and South constructed an international image of SMP proliferation among users, framing platforms as being dependent on the South for sustained profitability. Considering SMPs' business motives and their relationship with the government, some highlighted a form of intertwined and mutually constituting relationship between the two. According to Tarun:

You can't afford to completely antagonise the government of the country which you work in. I think two different accents, all of them try to defend free speech, have conversations with them, to be able to push back on certain things, like they all try to different degrees [...] It's pretty clear in their dynamic who has the power - obviously, the government. But that doesn't mean that the platforms are completely saying 'okay, just give us,

like every day you can send us one PDF, [...] that will do', it's not there either [...] If you have a government that has the power to ask for any content to be taken down sometimes you need to have a good relationship with them to convince them that certain content should not be taken down.

Reminding us of the power dynamics between SMPs and the government (see Part 6.2), the language Tarun used here aligned with Ravi's statement on the need for platforms to maintain 'a good relationship' with the state, while also emphasising their capacity to decide and act against government requests. Notably, it also indicates a certain level of checks by the SMPs on the government requests. As Deepa put it:

I think both of them are acting as a check against each other, which is really interesting to analyse. The government obviously regulates each and every facet of society. So obviously it is acting as a check against what's happening on these platforms; these platforms are following existing laws in India and are following their own policies [...] But these platforms are also acting as a check against the government in the sense that they basically provide a very easy and a very strong avenue for criticism. And any criticism of the government which gains traction on social media which is covered by media houses acts as a check against them and they have to respond, and if anything becomes a public concern, they obviously have to respond on that issue [...].

Deepa's comment constructs a cyclical dynamic in which the government regulates platforms, while platforms act as a countercheck by amplifying criticisms against them. This illustrates an interplay between SMPs and the government, while also highlighting the role of users within this complex engagement.

Overall, my respondents offered differing perspectives about the government's relationship with platforms and SMPs' business nature. Their statements not only provide primary interpretations of the situation in India but also complement my quantitative analysis by offering contrasting insights. Although the SMPs' transparency reports show that Twitter removed more content than Facebook (see previous subsection, 7.2.1.1), my respondents portrayed Twitter as having a more critical relationship with the government than Facebook, which they described as maintaining a closer relationship with the government. This

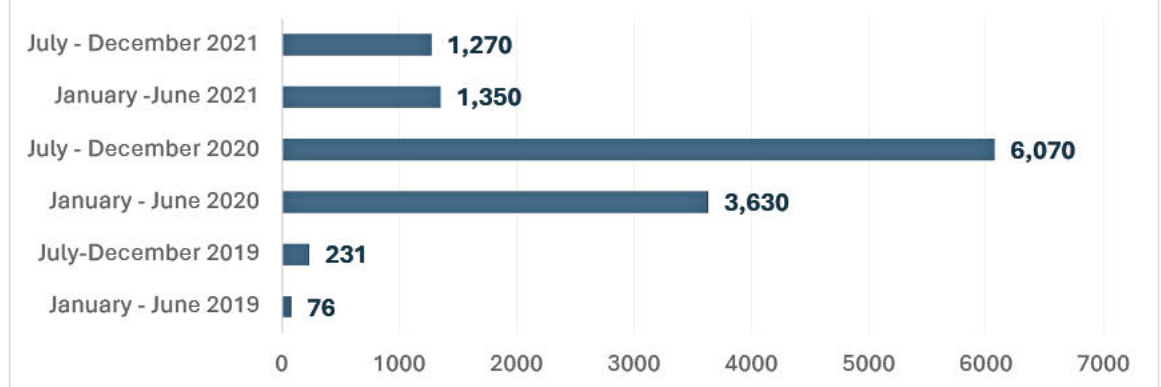
indicates that their perceptions were shaped less by numerical evidence and more by the narratives framing the relationship between platforms and the government.

7.2.2 United Kingdom

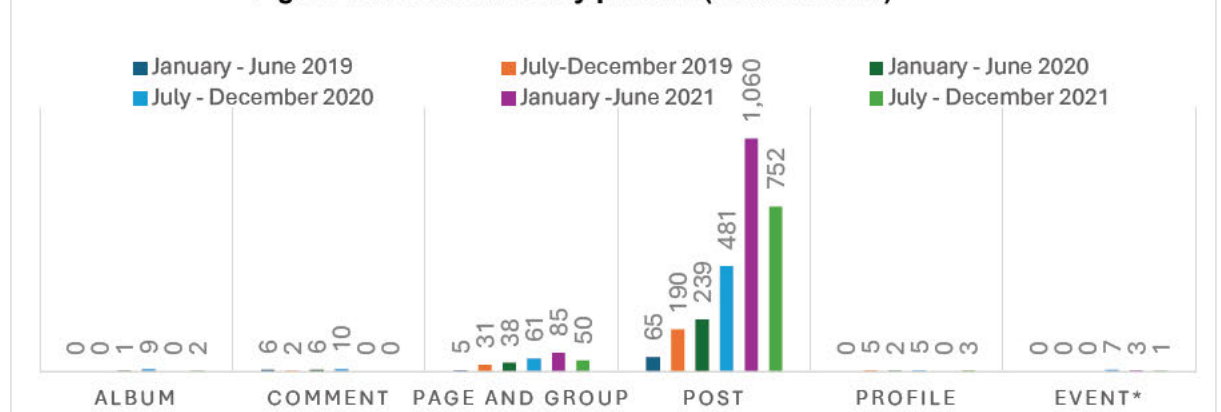
7.2.2.1 Transparency Reports

This subsection analyses content restrictions on Facebook and content removal requests on Twitter in the UK. Through this, it considers how platforms function as structures and agencies within the multi-stakeholder environment of digital governance.

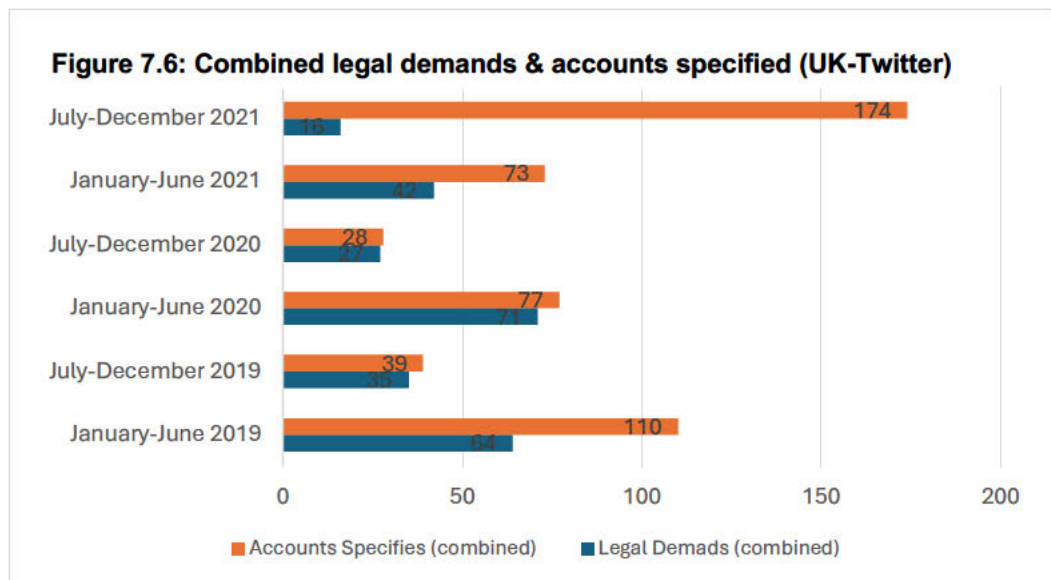
Given Facebook's unique approach, I analyse the total number of contents and products restricted under the law in the UK. First, as Figure 7.4 shows, Facebook restricted a total of 12,627 pieces of content between 2019 and 2021. The lowest number of restrictions was 79 during January-June 2019, while the highest number was 6,070 in July-December 2020. This means that Facebook restricted an average of 2,104 pieces of content every six months in the UK. When compared to the government's user data reports on -veillance (Subsection 6.2.2.1), the platform restricted less content (12,627 contents) than provided user data (60,815 accounts) to the UK government between 2019 and 2021. This indicates that the UK conducted more dataveillance than content control on Facebook.

Figure 7.4: Amount of content restricted based on local law (UK-Facebook)

The latter analysis focused on the type of content restricted, which the platform referred to as products. This provided a detailed explanation of the six types of Facebook content restricted in the UK, as shown in Figure 7.5. Based on the platform's six biannual reports, the most restricted product was posts - 2,787 in the period under study. This was followed by 270 pages and groups, 24 comments, 15 profiles, 12 albums, and 11 events being restricted on Facebook. This not only illustrates the ranking of the types of content restricted in the UK but also narrows down the area where most content control operations happened on the platform.

Figure 7.5: Restrictions by product (UK-Facebook)

Following Facebook, I analysed Twitter reports based on the combined legal demands received from the UK and its compliance rate between 2019 and 2021. Combined legal demands refer to court decisions and other legal requests made to the platform by UK officials. As shown in Figure 7.6, Twitter received 255 legal demands for 501 accounts. Unlike India, the UK's highest and lowest demands and accounts differed in biannual reports published by Twitter. The UK made the lowest number of legal demands, 16, during July-December 2021 and the highest legal demand, 71, during January-June 2020. Overall, the average was 42 legal demands for 83.5 accounts every six months. However, since Twitter did not comply with all the demands, I analyse its compliance rate next.



The compliance rate is the percentage of content removed by Twitter in response to the legal demands received. Before calculating the number of removals with the compliance percentages, it is important to clarify that Twitter did not provide its first biannual period, January-June 2019, as presented in Table 7.3. Based on their remaining reports, Twitter removed 135.8 of the 391 requested⁷⁴ accounts within 2.5 years, making an average compliance rate of 32.9% by Twitter to the legal demands made by the UK.

⁷⁴ 501-110 (January-June 2019) = 391.

Table 7.3: Compliance rate of Twitter-UK						
India-Facebook (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July-Dec 2021
Accounts specified (combined)	110	39	77	28	73	174
Compliance rate	0%	25.7%	32.4%	33.3%	35.7%	37.5%
Number of accounts removed		10.023	24.948	9.324	26.061	65.25

The above analysis reveals that Facebook removed more content than Twitter in the UK. Considering the different approaches of the two SMPs, my findings on Facebook might indicate the role of local law, since that was used to restrict content. Meanwhile, Twitter's low compliance rate (32.9%) can be interpreted as the platform following of its own structural process and its capacity to act otherwise to the legal demands received in the country. Nonetheless, both SMPs' content removal rates were lower than the number of information requests they received from the UK government ⁷⁵ (see Subsection 6.2.2.1).

7.2.2.2 Assessing the Role of SMPs' on Content Control

This subsection highlights my respondents' assessments of SMPs' role in content control in the UK. I present these in two points: SMPs as businesses and their significance for the government.

First, some respondents viewed SMPs as businesses operating in the UK. According to Tom:

⁷⁵ Facebook complied by providing 60,815 accounts to the UK government; Twitter complied by providing 1,924 accounts to the UK government.

[...] I would not say it's a relationship; it's more like platforms want to operate; they want to make money in order to do this. Of course, they need to have friendly governments that don't basically enact regulation that could crack down on them. As a result, they don't particularly care about enforcing human rights and doing kind of what the UK government tells them to bring down war comments, they will bring them down.

Tom's view reminds us that SMPs are not advocates of human rights but instead are businesses that seek to build profitable relationships with the government.

One example that can expand this argument was given by Lauren:

Facebook is going to listen to the big states, it's going to listen to the US, it's going to listen to Germany, it's probably going to listen to the UK as well, if there are certain things that they want content removed or groups to be silenced. [...] Facebook has made it quite clear that they're going to listen to that and negotiate on that level. So, I don't know exactly how it's happening, and I don't know the degree to which it's happening, but I'm fairly certain that it's happening. I think we can be sure.

Lauren's reference to 'big states' depicts a hierarchical grouping among states, which, as she suggests, shape how platforms interact with them. Although Facebook's collaboration with the government was not evident, she demonstrated a belief that such collaboration was happening with the UK.

Second, some respondents examined SMPs' role by focusing on the government. Anna argued that: 'Governments have always liked large companies running things because they can make a deal with a large company, that large companies of a similar size to the government understand each other'. Like Lauren's view on 'big' states, Anna distinguished 'large' companies in her example, complementing the power dynamics of the multi-stakeholder environment in the digital sphere. From a different perspective, Jessica viewed their engagement as a form of collaboration, not a hierarchical power relationship where the government was superior to the companies:

I think that the relationship between these big platforms and these companies is something that makes them less in a position to be able to kind of regulate them. We know that the government is collaborating with Facebook. We know that the government has different projects with Google for example, when it comes to the NHS. So then when it comes to actually regulating them, they're quite lenient [...] So I think a lot of the time the government doesn't really develop rules that are fruitful for

citizens. And because they collaborate with these big platforms and other avenues, then they don't really have an incentive to regulate them properly.

Jessica's account framed the government's collaboration with platforms as negatively affecting citizens. She argued that such collaboration prevents the UK government from 'proper' regulation. This supports not only the -veillance findings presented in Subsection 6.2.2.2, but also the wider lack of public trust - only 34% of adults - in the government's responsible regulation of emerging technologies (ONS, 2024; see Subsection 6.2.2.2).

Overall, my respondents' insights into the business nature of SMPs and their relationship with the government underscore the power of these platforms have accumulated, making them equivalent actors to state power. Reflecting the multi-stakeholder character of the digital sphere, this narrative highlights both the structural and agency roles of SMPs and raises concerns about how this might influence agency in terms of content control, particularly through inadequate regulation or having collaborations that are not centred on users.

7.3 The Legal Frameworks on Content Control

7.3.1 India

7.3.1.1 Individual Rights in Relation to Content Control

This subsection examines the thematically identified right to the freedom of speech and expression to understand how India's legal framework protects and defines individuals' capacity to act with respect to content. Indian citizens have the right to freedom of speech and expression under Article 19.1.a of the Constitution. However, the 1963 Amendments to the Indian Constitution limited this right under Article 19.2, signifying that freedom of speech is not an absolute right in India (Constitution (Sixteenth Amendment) Act, 1963). While this indicates the constitutional recognition of freedom of speech as a citizen's right,

its limitation demonstrates the extent to which it can be curtailed by other legislation in place, as analysed in the next subsection.

7.3.1.2 State Legislation Governing Content Control

This subsection investigates how law is constructed and structured around content control in India. It reviews three frameworks thematically identified from my FoN data analysis and supports them with secondary sources, when necessary. These are the Copyright Act, John Doe Orders, and the allied rules of the Information Technology Act. Given their distinct functions and purposes, I discuss them in two categories.

The first category involves legislation about the protection and regulation of copyrighted content. The Copyright Act (1957) covers the rights of intellectual property owners. It explains ‘When copyright is infringed’ (Section 51 of the Act) and prohibits the selling and spreading of copyright content (Section 63 of the Act). It defines the extent to which a copyright breach is considered criminal and outlines offences, not only for individuals but also for intermediaries who spread that content. The Copyright (Amendment) Act of 2012 further clarified intermediaries’ responsibility through a formal notice-and-takedown mechanism when limiting access to the copyrighted material (Prakash, 2012 and Copyright (Amendment) Act, 2012, as cited in India-FoN, 2016-21). This positioned intermediaries, including SMPs, as responsible actors in copyright control, involving them more directly within India’s enforcement system.

John Doe Orders are content-oriented legal remedies that allow courts to order blocking even when defendants are unknown (Ganz, 2012, as cited in India-FoN, 2016-21). Often employed against anonymous internet users (Gadodia *et al.*, 2023), these orders may require service providers to block a website’s URL (Padmanabhan, 2014, as cited in India-FoN, 2016-2021). My FoN analysis highlights judicial concerns by the High Court Judiciary of Bombay about John Doe Orders and possible over-blocking resulting from them (Chawla, 2015, as cited in India-FoN, 2017-21). For example, the Delhi High Court not only ordered several piracy websites to be blocked but also allowed re-directed domains to be blocked in 2019 (Joshi, 2019, as cited in India-FoN, 2019-2021). This supports the

concern highlighted by the High Court Judiciary of Bombay, providing an example of how such remedies may result in disproportionate blocking. Together, the Copyright Act and the John Doe Orders construct a legal framework in which SMPs are both regulators and regulated actors in copyright enforcement in India.

The second category involves legislation governing intermediary liability and government control over online content. It consists of two allied rules of the Information Technology Act of 2000 (IT Act): the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 (also called the ‘Blocking Rules’) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (‘IT Rules’).

The Blocking Rules allow the Indian government to request the removal of content from intermediaries. These requests go through a multi-step process overseen by a review committee consisting of a ‘Designated officer as its chairperson and representatives, not below the rank of Joint Secretary in Ministries of Law and Justice, Home Affairs, Information and Broadcasting, and the Indian Computer Emergency Response Team’ (see Rule 7 of the Blocking Rules, 2009). While this outlines the state’s procedure and the actors involved in content requests, Rule 8 requires service providers to either refuse or comply with these requests within 48 hours (Blocking Rules, 2009). Together, these rules establish a duality between the Indian authorities and intermediaries regarding content control, defining the structural role of law. This interaction, however, raises transparency concerns, as Rule 16 of the Blocking Rules (2009) guarantees the ‘strict confidentiality’ of requests and complaints. Such confidentiality shapes the public’s knowledge, which, in turn, illustrates a triadic relation between structure, technology, and agency in the context of content control in India.

The IT Rules (2021) introduced major changes to content control in India by establishing a regulatory mechanism for intermediaries, including ‘significant social media platforms’. By ‘significant’, it refers to SMPs that have more than 5 million users (India-FoN, 2021). At the time of the Rule’s enactment, both

Facebook⁷⁶ and Twitter⁷⁷ had more users than that limit (Basuroy, 2023c; Basuroy, 2023a). My analysis of FoN data highlighted three effects of this Rule on content control.

First, unlike the reviewing committee under the Blocking Rules (2009), the IT Rules (2021) allow courts and authorised government agencies to directly request takedowns (see 3.1.d and j of IT Rules, 2021). This established a direct engagement between authorities and platforms. The same provision also shortened the compliance period from 48 hours to 36 hours (3.1.d of IT Rules, 2021). This rapid timeframe leaves little or no time for appeals, pressuring SMPs to respond to such orders quickly, reinforcing the state's control over digital governance.

Second, the IT Rules require significant SMPs to have three officers - a chief compliance officer, a nodal officer, and a grievance officer - who are resident in India. Their responsibilities include ensuring compliance with state requests, being available at all times to work in coordination with the legal bodies, and resolving disputes and complaints received from the government (see 4.a to 4.c of the IT Rules, 2021). Non-compliance with these requirements make SMPs liable under Section 7 of the IT Rules (2021), subject to potential punishments under the IT Act (2000) and the Indian Penal Code (1860). This framework illustrates legal pressure from the government through the law on SMPs, as discussed in Twitter's case in Subsection 7.2.1.2.

Third, the IT Rules 2021 mandate SMPs to deploy automated moderation as a pre-emptive tool for content removal in categories like child sexual abuse (India-FoN, 2021; see Section 4.4 of the IT Rules, 2021). However, the issue of automated content removal becomes even more complicated and problematic considering the broad list of definitions given in Sub-clause 3.1.d (IT Rules, 2021). This not only raises the risk of over-removals but also affects individual rights, such as users' freedom of expression and the right to access information. Together, the allied rules under the IT Act establish a broad framework

⁷⁶ Facebook had 422.48 million users in 2022 in India (Basuroy, 2023a).

⁷⁷ Twitter had 23.6 million users in 2022 in India (Basuroy, 2023b).

governing intermediaries, liability, and outlining the scope of state authority over content takedowns.

Overall, by examining content control mechanisms through copyright mechanisms - the Copyright Act and John Doe Orders - and broader regulatory frameworks under the IT Act, this review underscores how existing legislation extends the power of government, integrates automated content control into India's governance, and generates issues of transparency and compliance pressure for SMPs. Together, these dynamics illustrate how legal structures construct and enforce rules in relation to technology and agency, while simultaneously being shaped by technological capacities and the practices of platforms and users regarding content control in India.

7.3.1.3 Legal Concerns About Content Control

Building on the public opinion data on trust in the court system outlined in Subsection 6.3.1.3, this subsection analyses three legal concerns raised by my respondents regarding content control in India. These are about the interpretation of the law, over-regulation, and de-prioritisation of individual rights.

First, some respondents were concerned about the interpretation of the law and its potential politicisation in practice. According to Tarun:

Like, imagine if the word is not widely defined, a government will not be able to order a piece of content to be taken down. But when the term is broadly defined, then it becomes the matter of interpretation of making a case [...] and then asking for it to be taken down when they need to. And I think it is definitely that this is a law [referring to the IT Rules, 2021] that we will probably pass once every five to eight years. Let's try to cover as much ground as possible and make sure that, even if it's vaguely defined, then someone will have to challenge it and go to court.

Here Tarun highlighted the paradox of having strictly and broadly defined laws regarding content takedowns, framing the latter as a way to maximise government interests by leaving them open to interpretation. He viewed laws as temporally adaptive instruments designed to address periodic concerns. From a

different perspective, Ravi commented on how the law allows the Indian government to takedown content:

The current government is very takedown-happy, and the IT Rules empower them to do so. Of course, the legal way is, where there's a tweet or post they don't like, they can get the platform to take it down.

By 'takedown-happy', Ravi meant the excessive requests the Indian government had made to remove content online. This was seen as a way of weaponising the law by those in power, as Tarun argued: 'I think laws and regulations are also logically weaponised by the people in power in order to further whatever agenda suits them, rather than protecting users from this kind of content'. The language he used, 'weaponising', emphasised the duality of law (like Amit cited in Subsection 6.3.1.3), showing how it can function as both protective and harmful, depending on how it is structured by those in power.

Second, some respondents mentioned over-regulation as another issue rooted in the law. For instance, Deepa highlighted the need for 'a distinction [to be] made between free speech and speech that can be regulated'. Acknowledging the need for regulation, she further stressed that 'it's very essential to remember that, while these platforms need to be regulated, over-regulation cannot happen'. Deepa considered 'speech that can be regulated' and 'over-regulation' as the extent to which she framed the boundaries of acceptable regulation. From an operational perspective, Priya discussed over-censorship:

So, in the world of regulation, sometimes it is over-censorship. The question is that there has to be balance over censorship. And platforms not handling fundamental rights of citizens, right? So, Indian Government right now is still getting a little towards those censorship, but again I would give them the benefit of doubt that it's also because they just don't know how to do it. [...]. And technology can never be politically neutral.

Priya distinguished SMPs from content governance responsibility, framing the government as having responsibility to protect 'fundamental rights'. Her perspective acknowledged the state's struggle to adapt to changing technology, suggesting that over-censorship may reflect institutional inexperience. Despite their different views, both Deepa and Priya agreed on the need for a more

balanced definition of what should be removed and what constitutes over-censorship.

Third, some respondents shared a concern about the de-prioritisation of freedom of speech in India, which contrasted with public opinion surveys. According to the Pew Research Center's 2019 report, 58% of Indians believed their right to expression was protected (Devlin, 2019). In spite of this, my respondents deemed the problem to be rooted in the case of *Shreya Singhal vs Union of India* (2015), where the Supreme Court had struck out Section 66A of the IT Act 2000 because it clashed with the freedom of expression guaranteed under the Constitution (India-FoN, 2016-2021). Section 66A was widely criticised for permitting arrests over offensive content (India-FoN, 2021) and for containing 'some very broad vague terms' (Tarun), raising the risk of criminalising free speech. Although this was a big win for Indian democracy and the protection of freedom of speech, its enforcement was problematic, as reflected in FoN reports from 2016 to 2021 and echoed by my respondents. Tarun argued that 'sometimes it's as simple as literally the copy of the law that the police station has is five years old, 66A is still there, they apply it [...]'. Thus, Tarun raised a communication problem in which law enforcement bodies are not up to date with judicial changes. Furthermore, Karan remarked that:

So, the courts have not always been the guarantors of internet freedom, and even in that decision where they strapped down Section 66A, they also upheld the government's power to block content, which is what they continue to use today.

Karan's point framed government actions in relation to Supreme Court decisions, offering critical insights into judicial functioning in India. Whereas his view also indicated concern about protecting the freedom of speech and expression, Deepa argued that 'if a person is targeted offline due to something that they have [...] published online, then that also affects the right to life and liberty, right to privacy, a lot of connected rights I guess'. Her view highlighted a domino effect on infringing individual rights resulting from content shared online.

Overall, the concerns my respondents recounted about the interpretation of the law, over-regulation, and de-prioritisation of individual rights comprised a common problem of democratic enforcement. This problem manifests through vague legal definitions, laws that permit over-censorship, or the continued application of a section removed by the Supreme Court of India. Another emerging problem is that they all place Indian citizens in a disadvantaged position, whether through divergent political interpretations, over-censorship, or being detained under a section that has been removed from the law. Together, my respondents' insights reinforced these problems about the legal frameworks and practices governing content control in India.

7.3.2 United Kingdom

7.3.2.1 Individual Rights in Relation to Content Control

This subsection examines how UK legislation protects individual rights in relation to content control and the extent of its application, to understand the legal structure surrounding agency. The UK guarantees the freedom of expression under Article 10.1 of the Human Rights Act (1998). However, like the right to privacy and freedom to access information examined in the -veillance theme, the UK considers freedom of expression to be a qualified right which can be limited for reasons listed in Article 10.2 (Human Rights Act, 1998). This means that, despite the legal recognition of freedom of expression, it is not an absolute right in the UK.

7.3.2.2 State Legislation Governing Content Control

This subsection reviews four laws regarding content control that I thematically identified from my data analysis of FoN reports: the Copyright, Designs and Patents Act, the Digital Economy Act, the Terrorism Act, and the Online Safety Act (with reflections on the Online Safety Bill). Due to their distinct focuses, I analyse them in three categories.

The first category involves two pieces of legislation about copyrighted and child sexual abuse content, which get interconnected at times. The Copyright,

Designs, and Patents Act (1988) play a key role in copyright enforcement; it allows the High Court to give orders to internet service providers in copyright infringement cases under Section 97.A. The Act further outlines infringements subject to criminal punishment - however, while it originally had a maximum penalty of two years' imprisonment, this was extended to ten years under Section 32.5 of the Digital Economy Act (2017). This extension in a newer act illustrates how legal structures adapt to changes and reconfigure platform obligations for copyright enforcement in the UK.

The Digital Economy Act (2017) provides a more comprehensive framework for content regulation. As also mentioned in Section 7.1.2, its Section 104 allows service providers to apply internet filters, as long as they fit into the providers' terms (Digital Economy Act, 2017). Additionally, my FoN analysis shows that Part 3 of the Act contains important provisions about online pornography, including access controls for children (Section 14.1), regulation of 'extreme pornographic material' (Section 22), and the requirement for an 'age-verification' procedure (Sections 16-17). Some of these sections were criticised in FoN reports for their 'poor definition and uneven application' (Gayle, 2016, as cited in UK-FoN, 2017-21), which aligns with one respondent's observation that 'age verification' could jeopardise privacy and personal security (Tom). This explains why the UK government dropped an automated age verification requirement to access online pornography in 2019, due to technical difficulties (Burgess, 2019, as cited in India-FoN, 2021). Triangulation using data from the House of Lords Library indicates that the amendment to the Digital Economy Act (Commencement of Part 3) Bill remained at its second reading phase (Brown, 2022) and was re-introduced as part of the Online Safety Act (2023). Although this highlights issues in enforcing automated age verification, it also illustrates the UK's continuing work to govern the digital sphere and tackle the problem of pornography.

The second category comprises legislation on the regulation of terror content. The Terrorism Act (2006) centres on terrorist activities, which include directly or indirectly encouraging the public towards terrorism through any statement, including those shared on SMPs. As discussed in Section 7.1.2, this law allows the Counter Terrorism Internet Referral Unit (CTIRU) to take down such content.

These takedown notices are issued by the power granted under Section 3 of the Terrorism Act (2006). A previous study cited in an FoN report showed that the CTIRU took down more than 310,000 pieces of material between 2010 and April 2019 (UK Counter Terrorism Policing, 2019, as cited in UK-FoN, 2021). This illustrates how the law creates a structure by empowering actors like the CTIRU to be a key player in content removal requests in the UK.

The third category entails legislation on content moderation and online safety. The Online Safety Act (2023) is the most comprehensive law on content moderation in the UK, designed to regulate illegal content and provide a safe online environment for children and adults. Drafting of this Act started in 2019, when the Department for Digital, Culture, Media & Sport and the Home Office published plans to increase online safety in their Online Harms White Paper (2020). However, FoN reports from 2017 had already noted government accusations against SMPs for their inadequate management of hate speech (Warrell and Murgia, 2016, as cited in UK-FoN, 2017), showing that the Act's rationale was influenced over time. The government consulted on the subject with industry stakeholders and civil society organisations between April and July 2019 and released a response in February 2020, which outlined its plans to regulate user-generated content on SMPs (Department for Digital, Culture, Media & Sport, 2020, as cited in UK-FoN, 2020). The Act came into force in October 2023, after I had completed my FoN and interview analysis. Instead of deleting three key findings I derived from the Online Safety Bill (OSB), I expanded my analysis with data source triangulation and investigated the change following its enactment.

One of the primary criticisms of the OSB was the 'legal but harmful' provision, which focused on removing content generated by users online that was not illegal, but was deemed harmful (Harbinja, 2021, as cited in UK-FoN, 2021). Although the next subsection expands on this with my respondents' views, the research briefing I triangulated from the House of Commons Library notes that the 'legal but harmful' provision was removed before passing the final Act to prevent potential over-removal and curtailment of freedom of speech (Woodhouse, 2023, p. 77). This change demonstrates not only deliberation on

‘legal but harmful’ content, but also the effectiveness of the consultation period and the legislature’s step to strengthen democratic principles in the UK’s digital governance.

Another important feature of the OSB was the prescription of automated content removal. It required the use of ‘accredited technology’ to remove terrorist and child sexual exploitation and abuse content (Harbinja, 2021, as cited in UK-FoN, 2021). Unlike the ‘legal but harmful’ provision, this requirement remained and was enacted under Sub-clause 121.2.a (Online Safety Act, 2023). To further regulate its application, the Act also empowered the Office of Communications (Ofcom) to regulate, ensure compliance, and issue fines or prosecution as an oversight mechanism (see Part 7 of the Online Safety Act, 2023). This framework illustrates a complex interplay in which the law embeds technological tools into its content governance while re-defining the duties of a traditional actor, Ofcom, to oversee its operation.

The last finding is in connection to the issue of age verification under the Digital Economy Act, where Section 81 of the Online Safety Act (2023) has established a procedural framework for verifying age regarding online pornography. However, this provision will only be enforced from 17 January 2025, which gives service providers time to make the necessary technical preparations (Online Safety Act, 2023). This not only illustrates a legislative adaptation to age verification technology over time but also highlights how the created legal structure requires re-shaping of service providers in turn.

Together, this review illustrates how laws on copyright, child sexual abuse, terrorism, and illegal content shape the UK’s legal framework for content control. Examining the relevant law - the Copyright, Designs and Patents Act, the Digital Economy Act, the Terrorism Act, and the Online Safety Act- highlights the adaptive nature of this framework, combining the enforcement of older legislation with the creation of new laws that address emerging challenges. These dynamics show how the legal structure both shapes and is shaped by technologies in governing the digital sphere.

7.3.2.3 Legal Concerns About Content Control

Building on the public opinion data on trust in the UK's courts and judicial system (see Subsection 6.3.2.3), this subsection analyses two concerns raised by my respondents on content control. These are the regulatory impact on individual rights and concerns about the Online Safety Bill.

First, they discussed the impact of content control regulations on individual rights, but from differing perspectives. Claire raised the UK's membership of the European Convention on Human Rights (ECHR), pointing out that it 'requires authorities to comply with international human rights obligations'. This emphasises that the UK is not only bound by the Human Rights Act (1998) but also with ECHR principles when restricting freedom of expression. Claire further questioned restrictions as:

So, there's the international rights of freedom of expression and the right to receive information. And restricting that right needs to be under very strict requirements and needs to be on a legal basis, it needs to be in the public interest, it needs to be necessary and proportionate, right?

Her references to 'public interest', 'proportionate', and 'legal basis' framed those rights as being qualified and subject to limitations under certain conditions. Anna, from a different perspective, argued that 'no right is in isolation, they all work together - freedom of speech, privacy, freedom from being interfered with, the freedom to protest, the freedom to assemble, these are all interlinked'. Anna's point emphasised the possible proliferation effects these legal infringements could cause for UK citizens, despite their legal basis and proportionality.

Second, some of my respondents shared concerns about the law-making process of the Online Safety Bill, before its enactment. Regarding the 'legal but harmful' provision, Claire asserted that:

If you start suppressing speech although it's legal speech, and you have the right to say things offline, but online it will get removed or the spread of it gets reduced actively, then that's a problem because these are protected speech under international standards [...] Even when it comes to illegal speech these are very often very complex questions, right? You

go to the court and say, 'Oh, this is defamation'. And the court takes two years and evidence to make a decision and then you go to the court of appeal, and the court of appeal returns to the decision. [...] And it is problematic that the state requires platforms, under the threat of liability, to remove, to make this assessment, and also be talking about a lot of content, right?

Claire's account demonstrated the shift in state-level and digital-level regulation of governance, underscoring the difficulty experienced online. Additionally, Claire shared her personal observations on the development of the Online Safety Bill:

It very much comes from this premise of there is bad content that circulates online, social media platforms now need to take action to restrict this bad content, even more so that the children don't see that content [...] Yesterday there was an inquest that started, like an investigation or two weeks' investigation because a teenage girl, about five years ago, took her own life after [...] she visited a lot of self-harm pages apparently on Instagram and in the last six months of her life she liked thousands of posts, and went on Instagram like 120 times [referring to the Molly Russell case]. So, she clearly had some sort of addiction, mental health problem. So, she committed suicide and that is a very prominent case that they always name when they say we need to make sure that our children are safe online, and that they don't get targeted and exposed to harmful content, and social media platforms need to take responsibility. [...] They're looking at imposing obligations, duty of care on social media platforms, so that they again identify and restrict and potentially remove content that is harmful [...].

Claire's example set out how the need for the law is socially constructed through media and securitises the issue in a way that creates a public interest. Her reference to 'we need to make sure that our children are safe online' illustrated how the digital sphere is discursively presented as a threat, while the regulations and obligations are seen as the solutions. Additionally, citing a five-year-old case highlighted a strategic re-invocation of the case at the time of the OSB. This stresses how public interest can be shaped around sensitive topics by the media.

Another concern my respondents expressed was defining what 'legal' or 'harmful' means under the law. During the Bill phase, the power to define 'legal but harmful' was listed as one of the duties of the Secretary of State, which was criticised by Richard:

[...] one of the fundamental problems with the proposed Online Safety Bill is that the Secretary of State was the one who would ultimately deem what was harmful and what wasn't, even if it was legal. The whole idea is that well, because you can say it at scale through social media it's harmful even though it's legal to say, and that is extremely dangerous. [...] It takes away the right of freedom of expression. And of course, as I've said, it undermines the right to privacy and to, if you like, the integrity of the human being. And your integrity is kind of invaded by both government agencies and also by companies.

Richard perceived vesting the power to define what is legal but also harmful to a person as problematic, arguing that it all influences citizens in the end. Claire argued that SMPs' increased responsibility to comply with this legislation could lead to platforms adopting a 'low-risk approach', where controversial content or legitimate content would be removed due to the fear of liability penalties and possible financial risks for service providers. Similarly, David commented that '[...] "legal but harmful" is just too vague a concept to leave it up to social media companies to decide what people can and can't say in the public square'. Altogether, these comments highlight a triadic concern about how regulating the technology could influence the people as a result, but only if that provision had passed into the final Online Safety Act in 2023.

In summary, my respondents shared their concerns about the impact of content control on individual rights and reflected on the 'legal but harmful' provision of the Online Safety Bill, which was later removed in the final Act. Both points centred on their broader concern that such laws restrict individual rights. This review illustrates the inadequacy of existing protections for individual rights and the infringements caused by state legislation when governing content control in the UK.

7.4 Experts' Concerns and Views on the Implications of Content Control on the Public

7.4.1 India

7.4.1.1 Awareness

My respondents raised the limited awareness of content control operations as one of the key challenges in India. Ravi addressed this by describing, in his view, how the government ought to be conducting these operations. He argued that they must be carried out with 'extreme caution', for 'limited use', with a 'well-defined sense of purpose', and under 'radical transparency'. While Ravi outlined an ideal scenario of what ought to be, Vikram and Karan approached it from observed practical challenges. From a policy standpoint, Vikram explained the situation as:

A lot of them [referring to the blocking orders] happen to be YouTube channels, and there are about four or five instances where such orders were exercised. And we know this because the government actually put out a press release saying that 'hey, we did this', which is also worth noting because the Blocking Rules [see Subsection 7.3.1.2] allow the government to have confidentiality. If they don't want to say, they often don't make the order public [...] There is one case where they actually went to the government and said, 'hey, you need to inform this person there's a takedown notice for their website', but citing security they say it's confidential and they don't make the orders public [...].

Vikram's interpretation suggested the government's selective transparency, framing disclosure as a tool serving its interests. His words on 'citing security' constructed a securitisation narrative where security justifies withholding information under the law. This aligned with the Software Freedom Law Centre (SFLC)'s RTI requests regarding 20 websites blocked by the government in 2019, which were denied under Rule 16 of the Blocking Rules 2009 but later disclosed by the MeitY in parliament (Mandhani, 2019 and The Print, 2019, as cited in India-FoN, 2020). This example resembles a similar pattern to the Pegasus incident, where the Ministry refused an RTI request and responded in parliament (see Subsection 6.1.1.2). These cases illustrate authorities controlled and selective approach to information dissemination and transparency under the powers vested in law in India.

Similar to Vikram's point on how government transparency affects public awareness in announcing takedown or blocking orders, Karan emphasised the Indian government's lack of transparency as an indicator of public awareness:

I would say that's definitely one of the biggest issues [...] when the government directly restricts content, those orders are not publicly disclosed, and there have been a few ad hoc disclosures in parliament [...]. I would say the vast majority of the public is not aware that the government is blocking content. And even when they do block content, there's no way for you to tell it's been blocked.

Here Karan highlighted that the public awareness of content removals depends almost entirely on government disclosure, framing transparency as a key determinant of how informed the public can be. Together, the Indian government's attitude towards RTI requests discussed above and its limited transparency reveal primary insights of how awareness is influenced in relation to content control in India.

Overall, while Ravi described an idealised account of how content control should operate, my analysis data from Vikram, Karan, and FoN reports showed that the Indian government provides limited transparency. This finding reveals the role of transparency in shaping public awareness, as restricted disclosure affects what the public can know about removed content. Together, these findings demonstrate how institutional practices, especially the legal frameworks surrounding content removal technology, constrain the extent to which the public can remain informed.

7.4.1.2 Impact on Specific People and Groups

This subsection addresses the people and groups my respondents identified as being specifically affected by content control. I have categorised them into four: political opposition, journalists, religious groups, and gendered experiences. Time-based data source triangulation determined that these groups started to be affected in 2017 (India-FoN, 2017), providing contextual background for the implications presented below.

First, my respondents highlighted those who do not support the BJP and their political values as a group that were influenced in India. One prominent case they mentioned was that of Aakar Patel, who is the former head of Amnesty International and a journalist (India-FoN, 2021). In 2019, Patel was prevented from travelling after the BJP filed a case against his social media comments about President Narendra Modi, alleging that they were ‘promoting disharmony among communities’ (Express News Service, 2022). Manish commented on this as:

I think the head of Amnesty International in India, I think his name is Aakar Patel, his passport was seized by the government, and they might have good reasons for doing that, but at the face of it what we know is that they were basically not OK with the kind of social media posts he was coming up with.

Manish’s view indicated that government disapproval of a post could be a reason behind Patel’s restricted freedom of movement. Although secondary sources confirmed that he recovered his passport in 2022 after years of court processes (Express News Service, 2022), his case is an example of arbitrary control on social media content by the Indian government⁷⁸ and its consequences on not only his freedom of speech, but also his right to travel. From a different perspective, my respondents reflected on how vague legal definitions of law enabled politicised arrests over social media posts. Referring to the IT Act, Deepa argued:

[...] because ‘obscene’ was not defined, what happened was that the police started using this provision to arrest people who were criticising the government. So, there was a person who was arrested in Uttar Pradesh because he criticised the chief minister of Uttar Pradesh. So that is one of the ways in which the government can actually target a person on these platforms - by filing criminal complaint cases against them, not just to regulate their speech, but also to make them an example, and to scare other people from also criticising them on these platforms.

⁷⁸ See Amit on the ‘arbitrary use of law’ in Section 9.1.1.

Deepa's point framed law as a weaponised tool for punishing critical voices and positioned the government as using such cases to construct a deterrent narrative that silences further criticism.

Second, my respondents identified journalists as a distinct profession that was affected (Priya, Sanjay, Amit, Manish, Karan). Priya mentioned the case of journalist Muhammed Zubair, also known by his Twitter username 'zoo bear', who had been arrested for his social media posts. Secondary sources confirmed that Twitter had taken down his posts for political reasons (TNM Staff, 2021) before he was arrested for 'promoting enmity' on the platform (Newsroom Staff, 2022). His case demonstrates the extent of the government's impact on opposition voices. From a legal perspective, Nikhil reflected on the use of anti-terror law against journalists:

[...] we've seen several journalists have been taken to jail on the basis of making a Facebook post criticising a political leader or an idea or an event. And in some cases, they've used anti-terror laws, like UAPA [the Unlawful (Activities) Prevention Amendment Act, 1967], which is a very strong anti-terror law, there are only 30 people in India who have had the UAPA put on them, and all of them are like the leaders or masterminds of actual prescribed terror groups. So, to add someone [a journalist] to that list who is making this Twitter post or social media post shows how they're trying to make people realise that whatever they say on social media platforms can and will be used against them.

Nikhil's reference to the use of anti-terror law against journalists illustrated the government's construction of their image as terrorists. His emphasis on the rare use of such laws revealed an extraordinary and unjustified link between real terror groups and journalists. This view complemented Deepa's point above, demonstrating the politicised use of law in favour of the ruling party, and the extent to which it can harm and impact certain professions and political opposition in India.

Third, my respondents named those who did not share similar religious values with the majority. According to Sanjay:

Okay, so the first thing that we have to keep in mind is that it matters what is the ideology of the government and what its priorities are. Now,

the ruling party in India has no interest in its development or in its holistic development. Development is only limited to the majority, which is the Hindu people belonging to the Hindu religion. [...] And when it comes to any sort of criticism [...] it's very touchy, it's very defensive, it wants to regulate and control everything.

Sanjay's account highlighted how religious differences construct inequality in India. He depicted Hinduism as a dominant force shaping regulatory practices. His observation aligned with instances of the government censoring TV programmes on Netflix, Disney, and Amazon Prime for religious reasons described in FoN reports (India-FoN, 2020). Together, these examples illustrate how religion shapes the structure's governance of SMPs and, in turn, conditions the experiences of other religious groups in India. Considering the BJP's Hindu values (see Sections 3.2 and 3.3 for context), this finding complements cases of political opposition and journalists, indicating that religious minorities are similarly affected on SMPs in India.

Fourth, my respondents pointed out how users' genders shaped their SMP experiences, particularly for women and LGBTQ+ users. Priya observed that women often needed to self-censor on social media: 'they think before posting, women especially they have a hard time because there's a lot of trolling, there's a lot of backlashes they see'. Hence, she framed gender as a factor shaping users' experience online. This further includes LGBTQ+ individuals and groups, as Deepa put it:

Nothing would happen to somebody who belongs to the majority and has expressed, for example, a controversial opinion, or somebody who is a heterosexual [...] However, for example, if you're gay or Lesbian, and especially in a country like India where it's still not as prevalent or as accepted as it may be in some Western countries, it can lead to a lot of backlash.

The language Deepa used illustrated gender and sexuality discrimination and the possible backlash that could follow social media activity. Her comparison with the West underscored the conservative norms that prevail in India. Together, Priya and Deepa's views revealed the role of gender and sexuality in determining the impact of content control experienced in India. Acknowledging the patriarchal values embedded in the state context (see Section 3.3), this finding

positions women and LGBT+ groups as also being negatively affected, like political opposition, journalists, and religious minorities in India.

Overall, this analysis addresses how BJP values dominate users' experiences on SMPs in India. It reveals how the political opposition, journalists, religious minorities, and gendered experiences of women and LGBT+ were more negatively affected than 'the majority'. The images my respondents constructed portrayed those holding critical voices, different or clashing religious beliefs, and being non-male justified backlash, pressure, and online abuse. Going further than ideological divisions, my analysis has identified the various subsequent risks experienced - online and offline - including travel bans, arrests, and backlash. These findings not only illustrate a triadic relation between technology and structure from agency lenses, but also complements the socio-political context provided in Chapter 3 from digital perspectives.

7.4.1.3 Self-Censorship

Acknowledging the debates surrounding SMPs and the Indian government discussed in Subsection 7.2.1.2, Edelman's (2022, p.15) public opinion survey showed that Indians trust neither the government nor the platforms. One outcome of this widespread distrust is a shared tendency toward self-censorship and the fear to exert freedom of speech. By self-censorship, I refer to users' pre-filtering and constraining themselves when creating and engaging with content on platforms, which in turn limits their own freedom of speech. While FoN reports from 2019 and 2020 described self-censorship as not yet widespread but a growing concern, the 2021 report noted the increasing influence of the BJP and legal practices in intensifying self-censorship in the country (India-FoN, 2019-21). To validate this decline over time, I examined earlier FoN reports, which confirmed safer environments with fewer self-censorship concerns evident in the country (India-FoN, 2016-18). One way my respondents explained self-censorship was through the 'backlash' users receive online. According to Vikram:

If every time you post something just by default you have a number of people abusing you, issuing death threats to your family, it is absolutely natural for someone to then start thinking twice about, either about how they phrase it or whether they post something at all, right? It's also worth

noting that this is not just restricted to abuse on the platform but there's also a tendency for law enforcement agencies to sometimes pick up posts that people put out and then actually pursue police cases [...].

Vikram's point illustrated how both online harassment and government backlash prompt users to self-question and tailor their online engagement. This demonstrates a triadic engagement in which platform dynamics and structural conditions foster users to self-censor, revealing both the constraints on agency and the reflexive thinking through which users re-configure their actions online. From a legal perspective, Karan viewed this as:

So, I would say that, with respect to the larger chilling effect I talked about, obviously the right to freedom of expression is being affected. And the individuals who are specifically being punished for the speech that they have said, with respect to them, obviously the restrictions are much higher because they've actually been arrested pursuant to their speech.

Karan underscored how the 'chilling effect' influences individuals' freedom of expression. He distinguished the broader chilling effect of the public from those who had previously been arrested for their online speech, suggesting that punitive experience intensify the extent of self-censorship. The link between this 'chilling effect and self-censorship' was also drawn by Tarun:

I think that its chilling effect and self-censorship are broadly the same in this context. People tend to not express themselves, or express themselves in a limited way, self-censorship happens. I think the chilling effect is the consequence to self-censorship rather in a way [...] whether you're a famous individual or a person with a big following or you're a small individual.

Here Tarun framed the act of limiting oneself as self-censorship, while describing its wider impact as a chilling effect. Beyond individual users, self-censorship has become a requirement for some organisations, as Sanjay explained:

There are policies in place where, let's say you are working for an organisation, the organisation will tell you that you have to be careful about what you post on social media, we do not want to be subjected to a lawsuit [...] Some do it formally while, say, you're joining a firm [...] But by large, most of the directions or suggestions come informally [...] This is

what I faced at my previous organisation [...] You will have people come in and tell you that, 'Okay, be careful what you post on social media, be careful of what you say, be less critical of the government, we don't want a lawsuit' [...] I don't think it comes from a place of bigotry or prejudice. It comes from a place of, all we want is to protect ourselves from a lawsuit.

Sanjay's experience shows how organisations have been influenced by the deterrent narrative of possible government action. His point revealed how self-censorship has been institutionalised in India.

Overall, my analysis highlights self-censorship as a form of protection used by both social media users and organisations against the Indian government's arbitrary power. This nuanced finding demonstrates not just public fear or distrust resulting from content control, but also how it restricts freedom of speech and online activity in India. It complements digital structuration by offering insights into how structural and technological conditions may create risks for agency, while also pointing to the reflexive processes through which users observe the digital environment and adjust their behaviour in response. From these perspectives, self-censorship can be understood as an expression of reflexive agency.

7.4.2 United Kingdom

7.4.2.1 Normalisation of Content Control

My UK respondents cited normalisation as a worrying outcome of content control operations in the country. One of the emerging arguments they raised addressed the social construction of law. In Subsection 7.3.2.4, I analysed the role of news in law-making through Claire's example of a girl with a history of engaging with self-harm posts online who had committed suicide five years earlier. From a similar rationale, Tom argued that the UK government normalises the extraordinary measures they enforce as:

The government here, they love to come up with a kind of like 'we think this is wrong', then 'we're going to fix it by then this thing'. There's just

going to be like a big announcement on TV, ‘this is the plan for the government to curb this, this is a very bad thing going on the internet, and ‘here is what we’re going to censor today’. And everything, of course, will be presented as world class, because here everything is world class or world leading, even though it’s not. I mean, just a huge PR opportunity.

Tom’s framing of it as a ‘PR opportunity’ underscored the role of media in normalising extraordinary measures and decisions. Both Claire and Tom’s points revealed the importance of social construction as a way to indicate how public views get shaped.

Another point my respondents raised concerned the public normalisation of infringements caused by content control in democracies. Claire approached this by focusing on the historical change in human rights:

[...] after the Second World War, obviously there was a big push for human rights [...] but I feel like now human rights is something that maybe people take for granted a bit too much. So governments all around the world have been happy to undermine first, say, post-9/11 it was more interested in responses to like what they said were ‘terrorism threats’ [...] disinformation, public health, safety of children really seems to be like the new thing where they are happy to impose a lot of measures [...] In the UK, we’ve had a lot of legislation that can be considered an assault on freedom of expression and people saying, ‘it’s the UK, not Russia’, or ‘we’re not in Zimbabwe, here it’s fine what they’re going to do’, but like NO! It’s also on the mindset and it slowly undermines democratic principles, and they’re all linked together.

Claire’s rationale highlighted how human rights have been gradually devalued and become negotiable, especially in the aftermath of major security incidents. She also critiqued narratives that portray infringements in the UK as exceptional compared to those in countries with authoritarian contexts. Having a similar view, Richard believed that such normalisation was blurring the line between democracies and digital authoritarianism:

I think we’ve become that [normalised] by default already, because all Western countries now use the same digital media platforms which are authoritarian in their operation. And Western countries that I know of are also introducing legislation which is to try to control these social media platforms. In other words, what they’re trying to do is to put more pressure or to make it a legal requirement if you like that social media

companies control the content which appears on their platforms, they're already doing that.

Richard's depiction of Western and authoritarian countries as being alike suggests that the digital sphere is governed through a single form of governance. His reference to law highlighted its role in creating a repressive structure that establishes control online.

Overall, my respondents shared two legal concerns - the social construction of law and public normalisation of infringements - in relation to content control in the UK. Laws that restrict individuals are socially constructed through the news to stimulate public interest (Claire), where they are presented as the key solution (Tom). Meanwhile, infringements of democratic rights are being normalised globally, mostly under a security rationale (Claire) and through content control on SMPs (Richard). Together, these views illustrate the normalisation of non-democratic content control and demonstrate the influence of law and technology on people.

7.4.2.2 Whose Freedom of Speech?

My respondents viewed freedom of speech as a broad concept that is applied subjectively in the UK. I categorise their views into three aspects - abusive behaviour, one-sided interpretations of freedom of speech, and subjective transparency - all of which raised the question, 'whose freedom of speech is being referred to?'

First, a journalist respondent, Anna, considered freedom of speech as something that could be used for abusive purposes by users online, asserting that 'I think thousands of people sending horrible messages to an MP just because she's black is abusive behaviour, I don't think that has anything to do with free speech'. Her opinion can be validated by FoN (2018), which reported that one-third of women MPs had experiences of 'online abuse, harassment, or threats' (Bradford University, n.d., as cited in UK-FoN, 2018). Anna expanded on her point by arguing that such freedom of speech should be limited to a certain extent:

So, the way I think about it is when you have hordes of people attacking somebody to silence them, that's not free speech, that's abusive behaviour. I think if we can separate behaviour and speech in that way, we can do a better job.

Anna's interpretation framed online harassment not as free expression but as a form of 'attack' that results in 'silencing' people. Her view reveals the need for a clearer definition of what free speech is.

Second, David pointed out the public's 'one-sided interpretation' of free speech in the UK. He argued that freedom of speech is not applied equally, especially on topics that are not 'fashionable' to the majority. He cited the example of Evangelical Christians' views on 'sexuality, gender, life in the womb, end of life care' as values shared by millions in the UK. However, opined that 'they don't get a fair outing and are viewed as minority views', further commenting:

So, I think that democratic debate presupposes that everyone gets their opportunity to have their say, and social media doesn't always allow for that. Because you also have this phenomenon of people weaponising the language of hate and weaponising mental health concerns. So, the weaponised language of hate by saying this opinion is hateful therefore must be stopped. It is not hate speech. When in fact it may just be an opinion you really don't like, but it's not actually hate speech, it's not actually calling for groups of people to go out and harm anybody on the other side. You just really don't like it. And the weaponised mental health concerns, they say 'hearing you say that makes me feel bad'. Now, I have a lot of sympathy with that feeling. But I don't sympathise with the idea that you write laws or algorithms to silence every opinion that makes you feel bad, because what's left, what will be left if we just do that? So that concerns me.

Here David suggested that dominant groups weaponise the language of hate and mental health to silence minority views. He framed claims such as 'hearing you say that makes me feel bad' as illegitimate and emotional grounds for suppressing unpopular opinions. Such subjectivity, as he argued, erodes democratic debate by constraining the space for dissenting voices. Having a similar concern, Tom highlighted the potential effects of the OSB on content shared by 'environmental activists or a political activist'. Together, these assessments illustrate some targeted impacts of freedom of speech for specific groups in the UK.

Third, a respondent, Lauren, highlighted the issue of subjective transparency in content moderation. Drawing on previous research experience involving SMP users, Lauren stated that ‘[...] people felt that the moderation policies were not at all transparent, they weren’t very evenly applied, and they were often very, very unjust’. Studying this through ‘the political culture in this country’, she asserted that the UK government tended to support right-wing content, while ‘more left-wing perspectives were much more likely to be shut down’. This observation is indicative of how political content gets shaped in the UK. Lauren further argued that these actions were taken without sufficient explanation from SMPs, as ‘sometimes things will just disappear, and they do not really understand why’. This concern aligns with wider public feeling about media, whereby 70% of people view it as biased (Electoral Commission, 2023). Together, these reflections underscore a broader concern about the inadequate transparency of content moderation and the uncertainty it creates in the digital sphere.

In summary, my respondents evaluated the influence of content control in relation to whose freedom of speech was at stake from three different perspectives - online abuse, one-sided interpretations, and subjective moderation. Their observations reveal distrust, polarisation, and division, where the majority’s freedom of speech hampers that of other groups. This highlights how structural frameworks, platform ecologies, and agencies’ use of SMPs can produce non-democratic implications and pose a risk to the equitable preservation of free speech in the UK.

7.4.2.3 Self-Censorship

Self-censorship⁷⁹ was the last way my respondents identified content control in the UK. One of the reasons they thought users self-censor was because they lack control over the content they share. Arguing that this lack of control creates long-term uncertainty, Jessica commented that:

[...] actually, a very small minority of people are posting, and the others are just not. On the other hand, because a lot of the stuff that is online is

⁷⁹ See Subsection 7.4.1.3 for my definition of ‘self-censorship’.

not going to be deleted and it can be used against you in multiple ways, then you censor yourself [...] But a lot of people are just more aware of the fact [...] so they are not saying that on social media, they might say that in private channels such as WhatsApp or Signal, where they feel more secure to kind of express themselves.

Here Jessica portrayed self-censorship as a form of protection and control for users. Her comparison of SMPs with more private channels like 'WhatsApp or Signal' depicted the different trust dynamics people may have on different platforms, showing a similar implication to the points made in my -veillance theme (see Subsection 6.4.2.2). Her view also resonated with Ofcom's (2023, p.12) public opinion findings, which reported that 48% of people expressed concern about potential long-term consequences of something they share online. Such widely shared concern reveals self-censorship as a reflexive decision for users to protect themselves online.

Another way that self-censorship was assessed was through increasing awareness about how the digital sphere works. Claire gave an example of this:

I saw recently in the New York Times [...] Don't ask me details ⁸⁰, but essentially, he took a photo of his two children, like small children. They were naked and they were siblings, and they were cuddling or something and he took a picture. [...] Google somehow scanned the content, because they were looking for pornographic content and deleted his Gmail account, and he didn't have access to anything [...] if people become aware through stories like that, that a lot get scanned; and they should be aware, because it's to protect themselves.

Claire's example highlights how negative incidents can potentially increase awareness, which might help people protect themselves online. Her emphasis on 'and they should be aware, because it's to protect themselves' indicates how she saw self-censorship as a rational and necessary strategy for navigating digital risks.

Overall, my analysis highlights self-censorship as both a consequence of limited technical control over shared content and a form of self-protection in the UK. It reflects a growing sense of distrust that prompts individuals to alter their online

⁸⁰ See the article by Hill (2022).

behaviours, control their own actions, and even limit what they choose to share online. From a digital structuration perspective, these dynamics offer insights into how structure and technology might shape user behaviour, while users' self-censorship can be understood as their reflexive monitoring online.

7.5 Conclusion

Content control was the second theme through which I investigated the digital governance of SMPs in India and the UK. Following this discussion of my analysis, the chapter can be summarised in seven points.

First, both countries take distinct approaches to controlled content topics, which is important for understanding their operations, construction of the law, and platform management. India enforces content control on a broad range of social, religious, and political issues, whereas the UK focuses on three main topics: copyright, terror, and child sexual abuse. While India's detailed list ensures consistency, it also opens up the risk of differing political interpretations (see Section 7.1.1 and Subsections 7.3.1.3 and 7.4.1.2). In contrast, the UK's categorisation appears more neutral, but cases like BT's Cleanfeed show how these categories get intertwined in practice (Section 7.1.2). Analysing these topics helped me contextualise how technologies were interpreted and integrated as operations within the multi-stakeholder environment of both countries, as explained in the next point.

Second, both countries have direct/centralised and indirect/de-centralised approaches in their content control operations (see Part 7.1). Despite differing categorisations in India and the UK, my analysis reveals them to have two tiers of operations. Direct/centralised operations concern those that are tied structurally to the government and its agencies, such as those contents removed under the law or by police. In contrast, the indirect/de-centralised approaches involve states' collaborations with other stakeholders, like through the pressure created on intermediaries in India and service providers in the UK. It also involves the integration of external tools into their governance, such as filtering

programmes in India and HateLab in the UK. Collectively, these findings underscore the complex interplay of technology with governments' structural engagement and the multi-stakeholder interactions in relation to content control. Complementing the first point, this not only reveals the interpreted use of operations within the two national contexts but also foregrounds the structure and agencies' interaction with technology in constructing digital governance.

Third, my transparency reports analysis generated significant findings for both my case study countries and the two platforms. They show that India⁸¹ removed more content from Facebook and Twitter than the UK⁸² between 2019 and 2021. While Twitter removed the most pieces of content (10,989) in India, the UK restricted more content under local law on Facebook (12,627). However, because Facebook and Twitter process content requests differently, I also compared the two platforms using their compliance data to assess how much content they removed across both countries. This comparison showed that Facebook had removed more content under the law (17,378) than Twitter (11,127) in both countries. Unlike Twitter's compliance procedures, Facebook's removals under local law demonstrated a higher potential for removing content in a country. This prevailing difference between the SMPs highlight their structural power to define content removal procedures within their own platforms, reminds us about their capability to act otherwise as agents, and the role of law which in turn influences them in the country they operate.

Fourth, my respondents from both countries assessed the role of SMPs, focusing on platforms and the governments. In relation to SMPs, they emphasised the importance of their country for platforms, either through the user market (like Indian respondents) or through state power (like UK respondents). Their views underscored SMPs' need to have a positive relationship with governments. Regarding governments, my respondents from both countries emphasised their need to regulate these platforms more effectively. These assessments led to a further finding of their intertwined relationship, as also noted by my Indian

⁸¹ 15,740 content items removed in India.

⁸² 12,765 content items removed in the UK.

respondents (see Deepa and Tarun in Subsection 7.2.1.2). This interdependency highlights the multi-stakeholder environment of the digital governance of SMPs.

Fifth, both democracies guarantee the right to freedom of expression, but this right is qualified and subject to limitations under the law. Although, unlike India, the UK also has an international oversight mechanism due to its membership of the ECHR, its ‘margin of appreciation’ doctrine allows flexibility in understanding individual rights restrictions under domestic legislation. While reflecting the structural consideration of individual rights in their legal frameworks, the qualified nature of the right to freedom of expression illustrates a limit to people’s capacity to act and be protected in both countries.

Sixth, both India and the UK have multiple laws regulating online content, covering areas like copyright, state security, public safety, and online pornography. Both countries passed new laws during my research period, such as India’s IT Rules (2021) and the UK’s Online Safety Act (2023), in addition to those that were already in place. This highlights the continuous and adaptive efforts of both countries’ legislation to control online content. Despite these developments, my Indian and UK respondents were in consensus about the de-prioritisation and infringement of individual rights within their respective countries. They also raised country-specific concerns, like over-regulation in India and the OSB’s ‘legal but harmful’ provision in the UK. Together, these findings provide core digital structuration insights into the construction of the law and the legal structure surrounding the management of technology, SMPs, intermediaries, and the public in relation to content control in the two countries.

Seventh, my respondents’ observations raised three different levels of observed implications of content control in both countries. At the general level, this comprised their shared observations about public awareness to content control operations in India and the normalisation of content control measures in the UK. From a more specific focus, they highlighted people and groups who are disproportionately affected compared to wider society. In India, this composed political opposition, certain professions (such as journalists), religious groups,

and individuals experiencing gendered backlash, while in the UK, respondents pointed to gendered experiences, and religious and political groups. At a more nuanced level, respondents from both countries mentioned self-censorship as a form of self-protection online, illustrating their own limiting of freedom of speech. Taken together, these analyses highlight the observed multi-layered effect on the public and people's reflexive monitoring of their actions in response to content control governance in India and the UK.

This chapter presented my research findings on the content control theme. The empirical findings presented on the socio-political context of content control operations, the role of SMPs, legal frameworks, and the observed implications on the public provide significant insights about the digital governance of SMPs in India and the UK. Reflecting on my digital structuration framework, the analyses detailed in this chapter demonstrates how the relative primacy of structure, agency, and technology shifts across different contexts of digital governance. This underscores their mutually constitutive relations and interrelated influence among each other. In doing so, this chapter makes a thematic contribution to my broader analysis of how India and the UK construct their digital governance in relation to SMPs, which I return to in Chapter 9. The next chapter presents findings on my final research theme.

Chapter 8 Shaped Discourse in India and the UK

Shaped discourse is the final theme of my research on digital governance of SMPs in India and the UK. This chapter presents my findings in four parts.

Part 8.1 presents shaped discourse operations and actors identified in each country from their socio-political contexts. It covers operations I thematically identified operations from FoN and interview data, supplemented by data source triangulation, such as reports. This analysis examines how shaped discourse related technology is used by multi-stakeholders and engaged structurally, informing us about the operations to which agencies are subjected in the context of India and the UK.

Part 8.2 examines SMPs' broader role in shaping discourse in India and the UK and specifically discusses Facebook and Twitter's tools and strategies in the two countries. It primarily draws on interviews but also enhances them with FoN and data source triangulation. Doing so addresses the structure and agency forms of SMPs through their relations with governments and the technological embeddedness within them.

Part 8.3 explores legal frameworks involving individual rights, state legislation⁸³ and government workings, as well as legal concerns related to shaped discourse. Drawing on FoN reports, secondary sources, and interviews, it highlights the documentary and operational methods adopted by the regulatory frameworks of both countries. Keeping my liberal internationalist position, this part considers the freedom of thought in Article 18 and freedom of expression in Article 19 of the Universal Declaration of Human Rights⁸⁴ (1948). As with earlier themes, the analysis explains the complex regulation of technology and agency by these legal structures.

Part 8.4 analyses observations and implications regarding shaped discourse on the public in both countries. It draws on my interviews, FoN reports, and data

⁸³ See Appendix 4 for legal extracts and notes on analysed individual rights and state legislation in both countries.

⁸⁴ See Appendix 4 for legal extracts and notes on the Universal Declaration of Human Rights.

source triangulation. In doing so, it examines the complex triadic engagement in relation to agency. Each part focuses on India and the UK in separate sections. Before presenting my findings, I define shaped discourse within the context of my research.

My research constructed the shaped discourse theme from two sub-themes, manipulation and targeting, as shown in Table 8.1. Manipulation refers to the spread of untrue or purposefully tailored information to mislead, impress, or configure the discourse. It is made up of codes including misinformation, disinformation, and doctored videos, among others. Targeting, by contrast, entails the employment of ‘manipulation’ tools in deliberate and possibly coordinated ways. These include - but are not limited to - bots, advertisements, and profiling. Together, these sub-themes form the shaped discourse theme, which I define as the spreading of manipulated content in a targeted manner. Like previous themes, shaped discourse exhibits dual-use characteristics that allow it to be used for both civilian and military purposes (see Subsection 1.2.3).

Table 8.1: Shaped Discourse	
Manipulation	Disinformation, misinformation, information manipulation, political propaganda, deep fakes, doctored videos, altered images, fabricated news.
Targeting	Bots, advertisements, targeting, profiling, payment to citizens/firms, cyber armies/troops, artificial boosting.

8.1 The Socio-Political Landscape of Shaped Discourse Operations

8.1.1 India

Based on my analysis, I identified two ways in which shaped discourse operations are conducted in India. These are political armies and private firms.

One of the most prominent methods that prevailed among all my sources was political armies⁸⁵, which are unconventional and non-militarised armies operating within their respective political parties. Having initially appeared in the 2017 report, my FoN analysis shows that political armies operated widely on SMPs, including Facebook and Twitter, where volunteers engaged in content activities related to their political parties, like posting, commenting, and liking, to help shape the discourse on these platforms (India-FoN, 2017-2019). As one of my respondents explained, their goal is to support their affiliated political parties while opposing other parties on SMPs (Vikram). This illustrates how the involvement of party politics at the state level influences shaped discourse operations online. The reason these political armies are considered an operation is because they coordinate and disseminate targeted information on SMPs. This approach not only blurs the line between an organic construction of discourse with manipulating and shaping of content, but also creates widespread public sentiment, as detailed below.

Political armies were popular in Indian politics, where both the ruling party (BJP) and the main opposition party (INC) had their own. According to the 2019 FoN report, an estimated 1.2 million volunteers were mobilised by the BJP, and 800,000 by the INC during the year of the general election. Despite their comparable numbers, my respondents emphasised the BJP's role more than the INC's. For instance, Vikram stated that the BJP was 'among [the] first to capitalise on this' [referring to the political armies], and Sanjay argued that the BJP had 'perfected how to deploy, how to manipulate, and how to sort of leverage social media to save the very discourse'. These viewpoints not only underline the BJP's dominance in digital operations but also demonstrate its mastering of politicised campaigns online. To explore this further, I validated the BJP's political army operation through secondary sources and found a report from the Oxford Internet Institute (OII): 'Country Case Studies, Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation'. This report cited a magazine interview with BJP's Head of IT Division, Amit Malviya, who described a political army as a 'nationalist group with Hindu warriors working to save the nation from break-India forces led politically by

⁸⁵ Also known as cyber troops, troll armies, and Information Technology Cells (IT Cells).

congress, communist and religiously by Islam and Christianity’ (Poonam and Bansal, 2019; Poonam and Bansal, 2019, as cited in Bradshaw *et al.*, 2021). This validation not only expanded on my interview data but also highlighted the intersection of the BJP’s digital operations with ideological polarisation in India. This finding underscores the state’s socio-political context and its influence on digital governance (see context in Chapter 3).

Following my assessment of political armies’ domestic activities, my analysis identified that they were also part of India’s international politics. A security analyst, Nikhil, shared his expertise on how Pakistani groups employed ‘extremely targeted propaganda, which was aimed at minority groups [...] explicitly calling on these individuals to take up arms’. This highlighted Pakistan’s strategic interference in the discourse in India. Conversely, the data source I triangulated exposed India’s interference in UK discourse during the 2019 elections. A report and a news article showed that this was being done by the ‘Overseas Friends of the BJP in the UK (OFBJP-UK)⁸⁶, who circulated messages in support of the Conservative Party and opposition to the Labour Party (Siddique, 2019; Siddique, 2019, as cited in Bradshaw *et al.*, 2021). Together, these two international examples show how political armies operate as tools of geopolitical influence in the Indian context, highlighting their dual-use capabilities to shape discourse in the transnational sphere.

The second predominant operation was the involvement of private firms in shaped discourse operations, including political campaigners and technology companies. Unlike political armies, this method illustrated a more professional approach and a diverse use of technology. One such operation was the NaMo app, Prime Minister (PM) Narendra Modi’s app. According to FoN reports, the app spread ‘misleading and inflammatory content’ in favour of the PM (Thaker, 2019, as cited in India-FoN, 2019) and was therefore classified as a discourse operation for its systematic use in propaganda. This finding was further evidenced by an active user⁸⁷ affiliated with the Silver Touch company, who was observed to be spreading propaganda on the NaMo app, while that same user was removed from

⁸⁶ See Section 8.1.2 for more details on their operations in the UK.

⁸⁷ ‘Indian Eye’ see Gleicher (2019) cited in Bradshaw *et al.*, 2019.

Facebook for violating its policies (which I validated through Gleicher, 2019, as cited in Bradshaw *et al.*, 2019). This case highlights both the importance of independent platform regulation and the role of private firms in spreading propaganda in India.

While validating my data on the NaMo app, I came across the Cambridge Analytica firm in Bradshaw *et al.* (2019), which enhanced my analysis of both India and the UK. My respondents raised concerns about the Cambridge Analytica scandal in the US and UK and discussed them mainly from the perspective of reducing trust in democratic systems globally (as discussed in more detail in Subsection 8.4.1.3). Although they considered this a Western phenomenon, the report assessed that Cambridge Analytica had ‘worked extensively in India’ (Crabtree, 2018, as cited in Bradshaw *et al.*, 2021) and named the INC party as its client. This finding highlights not only the global narratives constructed around Cambridge Analytica’s operations in the West, but also its involvement in Indian politics.

In sum, my analysis foregrounds political armies and private companies as two types of shaped operations that also involve SMPs in India. Identifying these operations also underscores political actors, like the BJP and INC, and companies, like Silver Touch and Cambridge Analytica, that engaged in the country’s digital context. Considering that both operations were constructed in a targeted manner, my analysis highlight the strategic and multi-layered shaping of the platform ecology and its possible politicisation by other actors, which connects this to the dual usability of shaped discourse operations.

8.1.2 United Kingdom

My thematic analysis found that shaped discourse operations were conducted by three different units in the UK: political parties, the British Army, and the OFBJP-UK group.

First, my analysis revealed two prominent ways that political parties shaped discourse during the 2019 election in the UK: disinformation and data-driven

campaigning. Disinformation operations by political parties varied, including creating and circulating doctored videos that contained false information. Unlike their originals, these doctored videos were processed and edited for manipulation or defamation, like one against the opposition Labour Party that was circulated on SMPs by the ruling Conservative Party (Kirka, 2019, as cited in UK-FoN, 2021). The data I gathered in validation from the OII report also noted that political parties, including Conservative and Labour, ‘employed overt disinformation to secure votes’ (Colley *et al.* 2019 as cited in Bradshaw *et al.*, 2021, p. 415). Regarding the main opposition, the same report revealed that Momentum, a group of 15 people associated with the Labour Party, had ‘produce[d] videos, memes, and other social media content’ (Satariano and Tsang, 2019, as cited in Bradshaw *et al.*, 2021, p. 415). These operations reveal how political parties, regardless of their position, employ various methods of disinformation in the UK.

Another way political parties shaped discourse was through data-driven campaigning. This method involved using collected personal data (see -veillance in Chapter 6) for political campaigning purposes. One of the most scandalous incidents that happened in the UK was Cambridge Analytica’s use of Facebook users’ personal data to target personalised advertisements during the Brexit referendum. While FoN reports from 2016 noted a higher volume of ‘leave’ content than ‘remain’ (Hermann, 2016, as cited in UK-FoN, 2016), the Cambridge Analytica Scandal was not uncovered until 2018 and continued to shape debates during my research. According to a researcher, Emily, the problem underlying such data-driven campaigning is that recipients ‘don’t ever get connected to the original political party’. Her point emphasised not only the role of data in shaped discourse for political purposes, but also the difficulty of linking these operations to political parties. Taken together, disinformation and data-driven campaigning highlight how political parties shaped discourse in the UK.

Second, my analysis identified the British Army’s involvement in SMPs in relation to discourse. This emerged from Emily’s recollection:

I went to a network event for people looking at elections and this guy turned up, [...] he was like, ‘Oh, I work in military operations to help target people with social media’. I didn’t even know that happened at the time, so I was like, ‘Oh wow’. And I feel like if he’d known I was a researcher, he would not have revealed that so quickly.

Emily framed the Army’s involvement on social media as both covert and surprising, revealing that targeting had already been integrated into military operations at a time when such technologies were not yet widely known. Since her experience was not a detailed account, I validated it through data source triangulation and found the report on ‘Ministry of Truth: The secretive government units spying on your speech’, published by Big Brother Watch (Carlo *et al.*, 2023). This report asserted the involvement of the 77th Brigade - a unit that conducts unconventional operations online - on monitoring discourse not only for international reasons, like watching Al-Qaeda or China, but also domestically. According to a whistle-blower, their domestic operations included monitoring what British people thought about issues such as the Conservative Party’s handling of the COVID-19 pandemic on Twitter (Carlo *et al.*, 2023, p. 64). It stated that the 77th Brigade has multiple units,⁸⁸ some of which cover operations specific to SMPs (Groups Within 77th Brigade, n.d.), confirming the British Army’s involvement in SMPs, as Emily had recounted.

The third type of operation I identified was international interference in the UK’s political discourse during the 2019 elections. As discussed in Section 8.1.1, this interference was facilitated through the Overseas Friends of the BJP (UK) (OFBJP-UK) group, as validated by my data source triangulation. The OFBJP-UK’s operations opposed the Labour Party, while protecting Conservative Party seats, as the group deemed that the Conservatives supported Hindu values and Indian political motives (Hundal, 2019, and Canton, 2019, as cited in Bradshaw *et al.*, 2021). This exemplifies not only international interference in the UK’s shaped discourse, but also the strategic integration of BJP-affiliated groups and their interests during the 2019 elections.

⁸⁸ Brigade Operations Centre, 5th Information Operations Task Force, 101st Information Operations Taskforce, and 6th Military Intelligence Battalion (see ‘Groups Within 77th Brigade’ in the bibliography).

Overall, my analysis identified three ways that discourse was shaped in the UK through political parties, the 77th Brigade, and the OFBJP-UK group. My findings reveal that these operations took place at politically sensitive times, such as elections and the COVID-19 pandemic, which underscores the importance of shaped discourse on digital governance. By highlighting operations conducted by different actors and the Army's structural adaptation, this analysis emphasises the technological dynamics of my structuration framework in the UK context.

8.2 The Role of Social Media Platforms in Shaped Discourse

8.2.1 India

8.2.1.1 Significance of SMPs on Shaped Discourse in India

The thematic analysis of my interview data uncovered four significant roles SMPs play in shaping discourse in India: information dissemination when compared to traditional media, transforming public communication and engagement, side effects of the discourse, and their power, as discussed below.

First, despite being viewed as a new form of communication, some respondents perceived the power of SMPs to be equal to, if not greater than, traditional media in India (Amit, Vikram). Vikram explained that one of the reasons for this was SMPs' 'low barrier', as anyone in India with an 'internet connection' and 'smartphone' could access the platforms, and thereby obtain information anywhere at any time. In spite of this ease of access, some respondents observed various problems SMPs created for the public, such as the lack of information accuracy (Nikhil, Tarun). Nikhil explained:

Another issue is that the differentiation between traditional news as well as reputable sources of media and information are slightly eroded because of the manner in which information is presented. And social media platforms, particularly in news feeds which would group together trustworthy and non-trustworthy sources in the same feed without being able to clearly distinguish or distinguishing between one or the other, for the user.

Nikhil emphasised the challenge of identifying accurate and validated information on SMPs. His comparison framed traditional media as a more reliable source of information, portraying SMPs as spaces where anyone can circulate content regardless of its accuracy. His view aligns with the CSDS-Lokniti public opinion survey (2019, p. 49), which showed that only 25% of respondents trusted the news they encountered on SMPs. This blurring of accuracy and distrust in information makes it hard to distinguish between true and false information, influencing broader discourse on the SMPs.

Second, my respondents claimed that the increasing popularity of SMPs had affected how the public engages and participates in political issues. In contrast to limited political participation on traditional media channels, some viewed SMP opportunities as revolutionary (Tarun, Karan). They explained this by pointing out how SMPs gave users ‘accessibility of public figures and politicians⁸⁹’ (Karan), and allowed them to share views and opinions with the masses (Priya, Amit). This meant that users were empowered to engage and express their thoughts on issues on SMPs, which is why some considered SMPs to be the new public space (Priya, Nikhil). Nikhil further explained this as:

I think that social media platforms can play a very beneficial role within a democracy in terms of acting as a digital public space within which individuals can gain information, express opinions, argue, debate with other citizens and reach consensus, and particularly within democratic politics, the ability for the citizens to engage in free and fair political debate and reach a consensus on something which is very integral for policymaking as well as for choosing your government as well, because consensus building obviously is very important. And consensus building within a democracy has to happen free of interference.

Nikhil framed SMPs as a ‘digital public space’, emphasising their democratic potential for citizens, while his point on consensus building stressed the need for it to remain free from interference. While this aligns with the discussion of my literature review on digital democracy (Subsection 2.1.2) regarding SMPs’ role in providing for a participatory democracy, it contrasts with public opinion surveys from CSDS-Lokniti on ‘Social Media & Public Behaviour’. Their findings reveal that the majority did not express a political opinion (54%), engage with such

⁸⁹ Such as ‘Twitter’ (Karan).

material (56%), or read news (47%) from SMPs (CSDS-Lokniti 2019, p.18). Despite these numbers of engagements, one respondent, Karan, believed that SMPs empower individual users to shape discourse:

[...] it [giving an example from Twitter] also gives individual users access to a much larger audience than they would otherwise have, compared to traditional media such as newspapers. So, I think to the extent that they allow ordinary individuals to shape the public debate in the public sphere, they definitely have some significant value.

Karan's comparison constructed the discursive power and capability of 'ordinary' users, framing SMPs as a space that empowers individuals. However, as discussed in the first point above, this not only creates the problem of inaccurate information, but also allows more uncertainties to flow around SMPs. Despite expressing divergent viewpoints, my respondents agreed about the revolutionising of public engagement and the diversifying of power in shaping discourse on SMPs.

Third, my respondents considered SMPs' power to have different importance for platforms themselves and for governments. From the platforms' standpoint, these shaped discourse powers helped build what Sanjay described as a 'money muscle', echoing the perceptions of other respondents who highlighted the financial motivations of SMPs, as set out in previous themes in this thesis. In contrast, some respondents emphasised that the Indian government was becoming increasingly aware of the power held by SMPs (Deepa, Sanjay). This awareness included not only the transformation of media and public engagement in SMPs, but also the power SMPs derived from their platform features. Respondents reflected on this by pointing to 'political advertising online, content moderation online and then direct restrictions by the government' (Karan), and 'micro-targeting, as well as targeted propaganda' (Nikhil). These observed operations validate CSDS-Lokniti's survey findings (2023, p.161) that 44% of survey participants receive advertisements based on their social media activities. This highlights SMPs' platform structures through their technological engagement and agency roles by underscoring their importance for the government.

Fourth, some respondents assessed the power of SMPs during the Indian elections, offering insights into the triadic influence of the country's political context. According to Sanjay, political parties in India had gained digital experience during the 2014 elections, learning that parties '[...] can shape the discourse through social media, the very nature of discourse can be influenced, can be manipulated through social media'. Similarly, Nikhil argued that this experience had helped parties to prepare for the 2019 elections, where SMPs had become vital tools for 'reaching out to voters', spreading 'political mis/dis-information', and 'target[ing] hate speech'. These views highlight the influence of platform ecology on voters, which can be further validated by CSDS-Lokniti's public opinion surveys in 2019. Their report reveals a connection between social media use and voting behaviour, showing that SMP users were more likely to vote for the BJP than other parties (CSDS-Lokniti, 2019, pp. 52-3). This underscores not only the dual-use character of shaped discourse and SMPs but also emphasises its politicised shaping in India.

Overall, my respondents' views on how SMPs challenge traditional media, empower individual users, create new challenges, and reshape political participation emphasised the transformative dynamics of SMPs in India. Moreover, their descriptions of the power of SMPs, from both platform and government lenses, offered shaped discourse insights about the multi-stakeholder environment of digital governance in the country, as contextualised in the election point. The next subsection discusses this discourse on Facebook and Twitter in more detail.

8.2.1.2 Facebook and Twitter

To assess Facebook and Twitter's specific roles in shaping discourse in India, this subsection starts by evaluating my respondents' views on their relationships with the government and then highlights platform-specific features that could be used to shape discourse.

First, similar to previous themes (see Sections 6.2.1 and 7.2.1), my respondents were in consensus about the closer relationship Facebook had with the Indian

government. Some explained this from Facebook's special offers to the BJP, like cheaper advertisement rates (Ravi, Amit). As Amit put:

[...] so, advertisements which are polarising, which generate more engagement, they would be charged less. And if something is charged less and it generates more engagement, then the advertiser is saving money. And they could put that money to hire more people to create more of that kind of content, right? And then, how does an algorithm read it, or decide what is more engaging? It would decide on the basis of likes we share or the engagements that we are generating, so then if you have an army to just engage with a certain kind of content, if you have an army which is putting like buttons on every content that they want to be sort of seen by the algorithm as more engaging, they can then game the algorithm. And somebody needs to be told, somebody needs to learn this procedure, and we know from the reporting and from the past that [...] Facebook works with the ruling party BJP, to train them on how to use the platform well. The result of which is that we have seen exponential growth of the ruling party on Facebook, and its contents' fidelity, which means that we have seen that the pricing for BJP advertisements was much cheaper than the other political parties in India.

Amit explained the strategy behind political armies and platform algorithms in shaping discourse. His note on the platform's 'training' of the ruling party indicates an exclusive relationship between the two, which further reveals a challenge to have fair digital governance and political competition in India. Another way my respondents viewed the ruling party's connection with Facebook was through the close relationship Facebook's former Public Policy Head⁹⁰ had with the BJP (Ravi, Nikhil, Vikram). Vikram observed that she 'intervened and prevented action being taken against a member of the BJP, for fear that it will affect their business in the country'. Considering the business nature of SMPs, Vikram emphasised Facebook's collaboration in shaping discourse with different clients in the country:

An example of this was a couple of years ago, Sophie Zhang, who was one of the whistle-blowers from Facebook [...] she observed that for some time it was supporting one political party, then, after some time, supporting another political party. That will tell you that it's likely a paid contractor type of activity that's happening, right, and so [...] not all of this is about politics, some of this will also be about money and about the financial motivation, irrespective of the cost to public discourse and the state of democracy in India.

⁹⁰ Ankhi Das.

The image Vikram portrayed here affirmed that Facebook's close relationship with the BJP may not indicate the platform's support for the party's politics or ideology, but rather a business-driven collaboration. Despite having different interpretations, my respondents depicted a close relationship between Facebook and the BJP during my research in India.

In contrast, my analysis reveals that Twitter's relationship with the Indian government was more distant than with Facebook. This was primarily based on Twitter's responses to BJP requests and government reactions to the platform decisions in turn. Vikram referred to the 2021 farmers' protest as an example, noting that Twitter did not comply with some government content removal requests on 'activists, politicians and journalists', and instead 'flag the tweet of a member of the BJP as having manipulated content'. I validated this through a news article by Singh and Conger (2022) which suggested that this resulted in Twitter taking out a lawsuit against the government over content removals. Despite Twitter's more critical stance towards the Indian government, Vikram further commented that 'Elon Musk was not particularly happy with this court case, because he believed it risked Twitter's third largest market'. Once again, this underscores the SMPs' business motive and intertwined dependency to continue their operations in the country. Another example addressed in the FoN reports was that Twitter had flagged tweets from BJP leaders as 'manipulated media' during the COVID-19 pandemic (PTI, 2020 and Bhargava, 2021, as cited in India-FoN, 2021). Taking an opposite approach to what Facebook's former Public Policy Head had done in a similar situation, Twitter's actions resulted in police officers visiting the platform's Delhi office to discuss the matter (Singh, 2021, as cited in India-FoN, 2021). Taking data from my respondents, the news article, and FoN reports together, this analysis indicates that the Indian government reacted harshly responses to Twitter's noncompliance and illustrates the platform's critical stance towards the BJP.

Second, both SMPs had technical and non-technical features on their platforms which allowed discourse in India to be shaped. In addition to its advertisements and gamification of algorithms pointed out in the above quote from Amit,

Facebook was also assessed as using inauthentic behaviours to shape discourse in India. Facebook defines inauthentic activities as⁹¹:

Inauthentic sharing happens when Pages engage in behaviour that artificially boosts views or engagement for the purpose of increasing distribution from Facebook. This includes coordinated, artificial distribution of the same content at high rates across multiple, seemingly different Pages. Inauthentic sharing can also be defined as creating many seemingly independent Pages or fake accounts to hyper share the same content (*Avoid inauthentic sharing on Facebook*, n.d.).

This definition highlights the coordinated engagement of thousands of volunteers in Indian political armies as a form of inauthentic behaviour, since their aim was to spread content to support their own political party and oppose others through mass operations (as discussed in Section 8.1.1). But at the same time, this created the problem of tracing these inauthentic behaviours on platforms because these were real users, as Vikram asserted:

IT Cells, who are volunteer driven, so there is no way to tie it back [...] this was organic activity, whether the platform was turning a blind eye to it or not. So, some of those questions are harder to answer.

His view positioned Facebook's inauthentic behaviour as part of political campaigning in India, suggesting that the platform is engaged in politicised actions. This interpretation can be supported by FoN reports and Facebook news, which recounted the removal of 687 items of content from the political armies of the INC Party, 15 linked to the Silver Touch company, and 321 pages reported as spam (Gleicher, 2019; Gleicher, 2019, as cited in India-FoN, 2019). What is interesting about these numbers is that, although the BJP had a higher number of political armies than the INC (see Section 8.1.1), Facebook's report did not contain any inauthentic behaviour number from the BJP. This observed gap in the platform's action also complements Vikram's earlier concern questioning whether 'the platform is turning a blind eye' to the Indian government.

⁹¹ The same definition applies for the UK as well.

My analysis further identified bots and trending topics as forms of discourse shaping operations in Twitter. A Twitter blog defines bots as ‘an automated account’, stating that these can be used for purposes like trading but also in harmful ways, which is why the platform considers them on a case-by-case basis (Roth and Pickels, 2020). Tarun described different types of bots, including ‘entertainment bots’ which could be harmless, while bots in the ‘context of democracies and governments are net harmful and used [...] almost explicitly for polarisation’. His remark not only complements the platform’s own definition, but also underscores its dual-use character. Tarun expanded on the use of bots in detail:

Bot accounts are very rarely used for primary communication, or primary outreach. They are more often than not used to either amplify certain posts or react to/attack other bots with comments that seem to make it look a particular kind of discourse is taking place [...] They are used to drive attention to an issue, drive attention away from an issue, within an issue, frame certain narratives in a particular way. Often done in a very coordinated manner where I think it's quite common to see the exact same post with the exact same wording, spacing, punctuation, marks, everything [...] So, because of those reasons, I would say they definitely are net harmful. Net harmful because they don't showcase legitimate people, the legitimate feeling [...] and they also tend to disincentivise posting things that are against people as well [...] And sometimes these bots also end up being coordinated where they take lots of other activities that people may have originally set up or established and then also bring things from elsewhere on the internet and use that to attack them and to vilify them or to bring up things from their past [...].

Tarun’s account framed bots as coordinated instruments of manipulation that shape broader narratives on the platform. His classification of these as ‘net harmful’ underscores how SMP engagements can be fabricated and mobilised to target voices, and once again highlights their dual-use capability for both good and bad purposes.

The other way discourse gets shaped on Twitter is through trends. Twitter has a ‘trending topics’ tab, listing timely and popular events and discussions for users. Karan suggested a link between bots and the creation of trends on Twitter:

If you go and you click on the trend and you start looking at the tweets, you'll realise they're actually only about five or six tweets, that the

content of those tweets has just been copied and is being tweeted at mass by hundreds and thousands of accounts. And you will very often see that is tied to a political event. So, some real-world politician would have given a speech, or they will be in some city, or they'll be in a particular campaign issue and then you will see that trending immediately on Twitter, and that's not authentic user engagement cause those tweets are just copy-pasted.

Like Tarun, Karan described how bots use exact copies of tweets in a coordinated manner, resulting in the creation of trends. His observation that such operations occur during political events underscores the dynamic and influential role that Twitter's trending lists play for users. This can be supported by an example from FoN, when both the BJP and opposition parties started hashtag operations through bots (*#TNwelcomesModi* and *#GoBackModi*) following Prime Minister Modi's visit to Tamil Nadu in February 2019 (DFRLab, 2019, as cited in India-FoN, 2019). Together, these two features of the platforms, bots and trends, highlight how Twitter shaped discourse in India.

In summary, my analysis identified several important roles Facebook and Twitter played in shaping discourse in India. These comprised not only the platform-specific features embedded in their systems, but also their socio-political stances when engaging with the Indian government. Observing the prevailing difference between Facebook and Twitter's relationship with the BJP (or the government broadly) indicated some state-level consequences that platforms might receive, like police visits to Twitter, when they do not comply with the BJP's politicised removal orders. This emphasises the Indian government's interest in establishing politically corrupt ties with SMPs when governing the digital, which comprised a valuable insight into the country's digital governance.

8.2.2 United Kingdom

8.2.2.1 Significance of SMPs on Shaped Discourse in the UK

This subsection presents three significant aspects of SMPs raised by my UK respondents regarding shaped discourse. These are: shifts in how information is

accessed, SMPs' power to direct information, and how platform features are designed to increase user engagement.

First, SMPs were seen to play a significant role in disseminating information and fostering discourse, especially when compared to traditional media. According to Lauren:

So, these environments [referring to social media] are immensely powerful in filtering and shaping and determining the information that we receive, and in many ways they're way more powerful now than the traditional forms of mass media or the broadcasting companies or the press. That's not to say they don't carry influence anymore, but it's a negotiation and certainly the mechanisms, the kind of landscape setting the conditions under which that information comes through set by social media platforms are immensely powerful in Britain, as in anywhere else, yes.

Lauren emphasised the need to reconfigure of the information landscape, stressing SMPs as a challenge to traditional media and as powerful actors shaping the flow of information. She further gave an example of the BBC's reliance on social media 'for filtering, for amplifying, for promoting its content', meaning that it has to adhere to SMPs' policies. This demonstrated not only SMPs' power in requiring other media channels to comply with them, but also that traditional channels, like the BBC, choose to publish their content on these platforms.

Second, some viewed SMPs as having the power to decide what they showed and to direct users' discourse. Differing from the content control operations discussed in Chapter 7, Claire shared her expertise by highlighting other unique ways in which this could occur:

[...] the power of social media to decide what we get to see for instance online, and in the end, information shapes our thinking, shapes our political views, shapes our musical tastes. So the power that they have through their algorithms and content curation and the recommender systems to decide on an individual level what I get to see, and also on a more societal level what is immense and not on a more wider level, I do think it's true when people talk about filter bubbles or confirmation bias, where you get reinforced in your views, because that's what you look for, so they know what you like.

Claire's reference to SMPs' 'algorithms', 'content curation', and 'recommender systems' highlighted SMPs' complex dynamics and their power to control what content users can see. Similarly, Mark remarked that SMPs are 'such a great reinforcer of preconceived notions', connecting people with similar views and distancing them from others:

I remember 30 years ago saying, 'the internet is fantastic, it will open up people's eyes to other viewpoints', and I remember standing up and saying, 'you could read a newspaper from any country in the world, isn't that fabulous?' And here we are 30 years later, and we've realised that actually, we're reading less. We don't have enough time to engage with all the different viewpoints, and so we seem very happy just to engage with people who, as I say, already think the same way that we do.

Mark's reflection portrayed a sense of disappointment about the loss of early hopes for the internet due to users' uncritical engagement despite greater access to information. Another example of SMPs' power over discourse was the growth of right-wing extremes globally, as Jessica discussed:

Yes, it shapes society in a collective way but also individually, me, Jessica, I don't see specific things on social media, but then I get a lot of fake news or conspiracy theories that could really direct me. They say that a lot of the flourishing of a lot of right-wing movements, it's not like these people didn't exist before, these opinions existed before, but social media has the power to amplify a lot of these ideas and that creates a more radicalised population because you are able to go into these filter bubbles where you are consuming that even further and that can affect you in different ways.

Here Jessica underscored the transformative effect of SMPs' amplification of pre-existing right-wing ideas, thereby increasing their visibility. Altogether, the views of Claire, Mark, and Jessica help explain how SMPs and their ecologies shape the discourse constructed on these platforms.

Third, my respondents addressed SMP features that increase user engagement. This finding was in line with the business nature of SMPs (as discussed in Sections 6.2.2 and 7.2.2), since respondents agreed that SMPs prioritised content that was engaged with more by users than ensuring such content is accurate. Richard commented that:

[...] of course, the companies themselves use a lot of algorithms that invade our privacy and are actually coercive. Machine learning in particular is used quite heavily in filtering of content, recommender systems and so on. You are probably well aware of the major technologies, algorithms if you want to put it more precisely, that are used for commercial benefit. And the commercial benefit is obviously to provide more targeted advertising. [...] the advertising revenue is about engagement, many of the algorithms are designed to keep users on the platform for as long as possible. And that's actually quite toxic. One of the problems that we've seen with fake news and conspiracy theories is that it spreads six times faster than genuine news, so that's good news for social media platforms and the business model that's the generation of revenue and profit. But it's not good news for society and for democracies as a whole. So, on one level private companies, social media companies, are already using technologies in a way that is detrimental to democracy.

Thus, Richard portrayed SMPs as spreading toxic content rather than facilitating the circulation of accurate information, driven by financial motives that ultimately influence society (this will be discussed more in Part 8.4). Similarly, based on her research experience and personal opinions, Jessica asserted:

I think that users are affected in multiple ways because the kind of stuff that you see and engage with on social media is very much dictated by the way that the algorithms are ordering specific content, but also the way that algorithms make connections between different kind of things. So that means that people's perceptions of what is happening is skewed and is affected by the decisions that are directing these companies and how they are showing us different stuff or filtering stuff. So that means that maybe we don't hear about specific important demonstrations or news or different information that is important for us about even COVID, and at the same time we get an amplification of fake news and misinformation, disinformation, because those kind of pieces of content and people receive more clicks and, as we know, more engagement means more money for these platforms. [...]. So that is a huge problem because that really shapes how we understand society, how I understand news, how I understand the important things in my life. [...]. But a lot of the time people think, 'oh, you know, it doesn't matter because algorithms are objective or because algorithms are neutral, and it depends on what you click'. But as research has shown [...] that is simply not true.

Jessica's account illustrated a disparity whereby users lack control over the content they are shown and assume that platform algorithms are objective. In explaining user engagements, both respondents highlighted the platforms' built-in mechanisms, emphasising how these technologies stimulate users' online participation.

My respondents' evaluations highlighted SMPs' transformational role in how people access information, raised technical features on how their structures determine what content users see, and reflected on platforms' ecologies to explain their significance in shaped discourse. Their perceptions indicated the structural integration of technologies on SMPs, which in turn constructed the platform users engaged. Following this general assessment of SMPs, the next subsection focuses specifically on Facebook and Twitter.

8.2.2.2 Facebook and Twitter

Based on my respondents' experience and expertise, this subsection analyses Facebook and Twitter's key features and then their discourse shaping activities in the UK.

My respondents agreed that advertising was a primary way that discourse was shaped on Facebook. They shared concerns about Facebook's advertisements since they 'target them [users] with personalised content or advertising' (Tom), but also 'Facebook gets lobbied by state governments all the time' (Lauren). Despite these concerns, some perceived receiving advertisements as a fair exchange. Tom explained this 'exchange' by discussing users in SMPs where 'you as a user are given a free tool, like communicating or posting pictures or whatever, and in return, we are showing you advertisements'. Similarly, Richard used a well-known expression to describe the transaction: 'we all think it should all be free, but there is no such thing as a "free lunch" [...] we are paying for it by selling our data, which makes huge profits for advertising companies'. Richard's use of the 'free lunch' metaphor illustrated the exchange between users and the platforms, framing SMPs' 'free' services as an illusion. While Lauren's approach explained advertisements from the perspective of state and lobbying interests, Tom and Richard viewed them through the lens of users, together constructing a user-platform dynamic in this specific context.

Facebook advertisements were also discussed in the context of the Cambridge Analytica scandal by my respondents. For instance, Lauren stressed the uncertainty that remained about 'the level of data actually collected [by Cambridge Analytica, and [...]] the degree to which political groups are getting

involved [...]'. This not only built on the concern about lobbying mentioned in the above paragraph, but also introduced doubt about the operation (which relates to the importance of indirect operations that are hard to trace back to their originator - see Emily quoted in Section 8.1.2). This was not to say that the advertising informed by Cambridge Analytica's data-informed targeting worked or failed, but to note that it interfered with discourse in a manipulative way, as Tom commented:

Which is a bit like what happened with Brexit here in the United Kingdom, [...] everybody had a different idea of what this means. Because everybody was receiving different messages and then people found out that actually okay, even though they voted for something, after that they got something else.

Tom's observation illustrated a complication arising from this interference after the referendum. Some of my respondents viewed this scandal as affecting Facebook's relationship with the UK government, especially when Mark Zuckerberg, Facebook's CEO, did not attend the questioning about Cambridge Analytica and stopped travelling to the UK (Mark, Jessica). Commenting on his absence from a parliamentary committee on Cambridge Analytica, Jessica stated:

The problem is that the power is still with the bigger companies. There are still investigations that are ongoing in terms of involvement of Cambridge Analytica and elections. And we just don't really know what is happening in the back end. So that also applies to the UK. And if you remember the DCMS asked Mark Zuckerberg to come, and he didn't come. So, their picture on social media is that empty seat. And that is showing how Mark Zuckerberg would go to different Congress or Senate hearings in the US, but he wouldn't come to other countries. Because they're just not that important, because they're not the ones who are regulating or restricting their practices in a way that really influences them.

Jessica's image of Mark Zuckerberg's 'empty seat' stressed his ability and power to refuse a state call, illustrating his agency and capacity to act otherwise. Considering that Facebook is based in the US, Jessica's comparison of Zuckerberg's probable willingness to answer to the US government while refusing the UK and other countries suggested that non-US states are less significant for the platform. This reaffirms SMPs as independent actors in digital

governance, while highlighting the shifting power balance and their complex relations with states in which they operate.

My respondents named several of Twitter's shaped discourse features: user-level campaigns, bots, and trends. Emily observed that 'Twitter changed their regulation to not allow political ads [...], which means they [users] can still do a lot of free organic reach on Twitter'. By pointing out this change, Emily stressed that still 'so much gets done [on Twitter] because you can have networks and influencers who are not paid advertisers, but they might just be supporting a campaign'. While this underscored Twitter's significance as a platform shaping discourse (see the previous subsection), it also illustrated non-technical discourse shaping by users (or influencers) in engaging with content on the platform.

Some respondents described the use of bots as a technical feature of Twitter. To explain this, I continue using the platform's definition of bots that was given in Subsection 8.2.1.2, but within the context of the UK. As Jessica put it, '[a bot] contributes in a variety of ways; I can't really say it's either positive or negative'. This demonstrates the potential dual usability of bots on Twitter. From a more political perspective, Lauren described bots' importance as:

[...] bots used well by organised parties could completely change the narrative on any topic. If it's done in a concerted way, they can absolutely flood the media environment, they can flood alternative perspectives, and they can amplify and push up to the top particular ways of seeing the world, and actually for use in political campaigns that's becoming increasingly common. I think looking at the Twitter content around Brexit, there was a study done that showed the amount of content that was coming from bots, which was really incredible. [...] because in the moment we don't really have time to assess it, a lot of people might say that sounds like a bot but we really don't know, right? [...]. So, it's incredibly important. I think bots play an increasingly important role, and the more they are collectively produced, the more they are algorithmically produced, the more influential they're going to be.

Thus, despite recognising their technical and collective production, Lauren emphasised how bots shape platform narratives and create uncertainties for users about whether tweets are accurate or coordinated. Her example of Brexit built on the Cambridge Analytica scandal involving Facebook, raising the

possibility that similar discourses may have extended to other platforms, like Twitter. Moreover, constructing links to both user-level engagements and bots, Lauren pointed out the role of the trends tab on Twitter:

So, to make a more sociological point I suppose we are socialised into thinking that what everybody else is talking about has importance, right? And that's what we should be talking about, that's what we should be thinking about. It [referring to the trends] gives it prominence in our heads in the same way that traditional mainstream media agenda setting did. So, we have a sense that these things are important and then other perspectives which just never appear, which never make it through, which are removed almost before anybody gets to read them. And that's very powerful and setting the boundaries and respect of acceptable, important public discourse. And absolutely it shapes it. So, removing content in some ways is almost as important as the amplification of what you are actually going to talk about, what you're allowed to talk about and what's deemed to be important in societies is given that importance by its prominence in this public space.

Lauren's sociological interpretation of Twitter's trends highlights how the platform constructs a hierarchy of topics, which in turn decides what users should perceive as important. Together, these reflections illustrate how platform-specific features play an important role in shaping discourse on Twitter.

In sum, my respondents offered political and social reflections on the two SMPs and their technical features when explaining the platforms' significance for discourse. Their assessments illustrate that both platforms had unique features built into their structures and produced diverse methods of discourse shaping. Moreover, although the scandal took place in 2016 and was revealed in 2018, the above analysis underscores the continued influence of the Cambridge Analytica scandal on how people perceive platforms in the UK. This not only reminds us of the social construction of digital governance within state contexts, but also of the dual-use features SMPs have in shaping discourse.

8.3 The Legal Frameworks on Shaped Discourse

8.3.1 India

8.3.1.1 Individual Rights in Relation to Shaped Discourse

To understand existing frameworks around protection and the capacity of citizens to act, this subsection examines three shaped discourse-related rights in two categories. The first category reviews rights that are guaranteed under the Constitution, while the second reflects on the absence of the right to free elections in India.

First, the Indian Constitution guarantees freedom of speech and expression (Article 19) and freedom of conscience and free profession, practice and propagation of religion (Article 25). These rights affirm citizens' rights and capacity for independent thought and expression; however, both are subject to limitations. In addition to the limitations discussed in Section 7.3.1, Article 19 (as well as other fundamental rights covered in Part III of the Constitution) illustrates a gap in safeguarding 'interference' with freedom of thought and information. This means that the information Indian citizens access is not protected from interference. Similarly, Sub-clause 25.2(b) of the Constitution specifies the enactment of laws that are specific to Hindu-related matters. This limitation not only challenges the ostensibly secular character of the state, but also raises democratic challenges, given the effects of Hinduism in religious groups and the political context in India (see Chapter 3 for the context).

Second, I reviewed Part III of the Constitution to ascertain India's comparability with my UK findings on the right to free elections, but found that it lacks any mention of that right. Instead, the Constitution has Part XV on elections, which vests power to control elections in an election commission (see Article 324 of the Constitution). Despite guaranteeing the right to vote, the absence of any explicit right to free election highlights a systematic gap in safeguarding democratic functioning and in constraining citizens' capacity to exercise their votes in a fair environment.

Although none of these three rights - freedom of speech and expression, freedom of conscience and free profession, practice and propagation of religion, and the right to free election - directly address shaped discourse, they collectively form a framework that reflects the conditional nature of freedoms in India. Building on these agency-focused assessments of the legal structure, the next subsection investigates the state workings and legislation relevant to shaped discourse.

8.3.1.2 State Legislation and Regulatory Operations Governing Shaped Discourse

My analysis of FoN data identified four legal mechanisms that explain how the structure around shaped discourse is formed in India. These are the Indian Penal Code, the Disaster Management Act, the Voluntary Code of Ethics for the General Election, and internet restrictions.

The first mechanism is the Indian Penal Code (IPC) of 1860, which is a criminal code that extends to online communications. The IPC focuses on discourse objectives and public order disruption on topics including ‘seditious’ (Section 124.A), ‘defamatory’ (Section 499), and statements seen to promote enmity or alarm (Sections 153.A and 505) (Indian Penal Code, 1860, as cited in India-FoN, 2021). What is critical about these topics is that they are vague in character and open to interpretation, creating the risk of mis-criminalisation of discourse. This concern was reflected during the farmers’ protests of 2021, as my data source triangulation shows; the International Federation of Journalists (2021), which is a global union for journalists, reports that journalists who criticised and opposed the government for undermining small farmers were detained and faced legal consequences under the IPC. This stresses the centrality of interpretation while positioning the IPC as a structural mechanism that defines the boundaries of criminal communication online.

The second and third mechanisms relate to the management of misinformation and disinformation in India. The second was seen in India’s management of the COVID-19 pandemic, where Section 67 of the Disaster Management Act (2005) empowered the government to regulate discourse (see Disaster Management Act,

2005). In 2020, the Supreme Court gave responsibility to the media, including SMPs, to disseminate verified information obtained from government sources (Rajagopal, 2020, Chatuverdi, 2020, and Bindra, 2020, as cited in India-FoN, 2020). This extended legal responsibility and risked potential punishment for circulating any ‘false warning’ under Section 54 (see the Disaster Management Act, 2005). One example of this was the arrest of a ‘health worker’ for sharing false information about the number of COVID cases in Rajasthan (India Today, 2020, as cited in India-FoN, 2020). The third mechanism was seen at the time of elections, when the Indian Election Commission created a panel and a ‘Voluntary Code of Ethics for the General Election’ in 2019 (India-FoN, 2019). This encompassed regulating misinformation on SMPs, including ‘Facebook, WhatsApp, and YouTube’ (Pradhan and Beniwal, 2018, as cited in India-FoN, 2019). Despite their different contexts, both mechanisms illustrate how the law not only defines regulatory measures but also involves other actors to govern information online.

The fourth mechanism is internet restrictions, a practice evident not only in 2019-2021, but also in previous years from 2016 onwards (India-FoN, 2016-2021). They function as an operational method to control shaped discourse. Based on my FoN analysis, I ascertained that they are conducted under the Indian Telegraph Act (1885) and the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules (2017). These laws provide the legal basis for the government to suspend communications and information transmission, which in turn interrupts the discourse. One incident that happened during my research was nationwide public protests against the Citizenship Amendment Act⁹², when the Assam state ordered telecommunication providers to ‘indefinitely shut down the internet’, and only restored it following an order from Gauhati High Court (Karmakar, 2019 and Banashreee Gogoi v. Union of India, 2019, as cited in India-FoN, 2020). This illustrates the state’s suppression to control the internet and its use of shutdowns as a reaction to protests criticising the government (see 8.3.1.3 for more discussion).

⁹² This took place to oppose the government for passing a law that religiously discriminated against Muslim people seeking citizenship in India in 2019.

Overall, this review underscores how the legal structure - the Indian Penal Code, the Disaster Management Act, the Voluntary Code of Ethics for the General Election, and internet restrictions - frames criminalisation, arrests, internet restrictions, and content removals to regulate online discourse. It also shows how the structure involves actors other than the state and controls technology within its frameworks. The examples provided in accordance with each mechanism raise a risk of politicised management and democratic accountability in India. They also emphasise the importance of discourse and communication, especially at sensitive times.

8.3.1.3 Legal Concerns about Shaped Discourse

Acknowledging the public opinion data on trust in the court system given in Subsection 6.3.1.3 above, this subsection analyses my respondents' two concerns on the regulation of shaped discourse and internet shutdowns. These are about the regulation of discourse and internet restriction.

First, some respondents highlighted the need to regulate discourse. Priya deemed the ability to access accurate information 'to be a pillar of our democracy, without information how do you challenge anything? And nowadays it's more disinformation than it's accurate information'. Her emphasis on 'nowadays' framed disinformation as an increasingly prevalent concern, positioning it as a contemporary challenge. Focusing on its governance, Tarun acknowledged that online discourse was not regulated and emphasised the difficulty of doing so:

[...] when there was the Citizenship Amendment Act protests. Those are times when it especially escalates out of habit [referring to disinformation]. And on content, broader manipulation, it's unregulated in its entirety. It's also very hard to craft regulation around it [...] I would rather it not be regulated because, if it gets too regulated, similar to the other two things [referring to content blocking and takedowns] I think it will be used to stifle legitimate speech or it will be used by the Indian government to mandate that platforms require online social media companies to give an ID before they create accounts and things like that.

Tarun framed discourse governance as a paradox: while recognising the dangers of unregulated disinformation, his distrust of effective regulation highlighted the

law as a tool that could curtail citizens' rights. His viewpoint anticipated similar issues regarding the use of law as set out in previous themes in this thesis, like restricting freedom of speech (see Chapter 7).

Second, some respondents criticised internet restrictions. Priya assessed them from a 'proportionality lens':

They're widely disproportionate, very widely disproportionate. [...] you have to look at everything from a proportionality lens. [...] According to the Supreme Court also, internet shutdown should only be implemented in the absence of a less restrictive measure. But here, they are just the first line action, which is completely arbitrary, which is completely uncalled for. [...] There has to be other alternatives that have to be explored, that have to be figured out to control online situations.

Priya's emphasis on 'proportionality' and the Supreme Court decision depicted an ideal democratic framework that was absent in practice. Her reference to internet restrictions as 'the first line of action' illustrates how such practice is normalised in India. Focusing on the anti-CAA protests and when the US President visited Delhi, Manish commented on the legitimate use of internet restrictions:

So, first and foremost, the governments are actually using an established law to shut down the internet in these protests. [...] there are no fixed controls against which you can assess a particular situation before imposing shutdowns [...] So, unless something has already respect to violence [something serious that makes it a necessity], I think it's unethical and unlawful as well to have those shutdowns in place. [...]. When Mr Trump visited India in 2020, while he was in the nation's capital, there were riots happening in Delhi at that moment because of misinformation that was spread during the CAA protest. [...]. So, the internet had to be curbed over there because people from both religions, be it the Hindu community or the Muslim, they were spreading and inciting violence. So yeah, I know it's an unpopular take, but I have to look at the grey as well. It's a popular thing to say that 'freedom of speech should be absolute', that's the acceptable thing I think, but I would say there needs to be reasonable restrictions, depending on which part of the world you find yourself in.

Here Manish framed internet restrictions as a context-dependent decision, basing his views on a nuanced 'grey' space between freedom and restriction. He portrayed them as necessary to curb 'violence' and 'misinformation' at

politically important times. His perception of internet restrictions as a measure of control highlights their dual-use character, in which they can harm society while also protect the state. This ‘dual-use analogy’ was discussed by Vikram:

I think we've seen all of these rights in some shape or form. And the dual-use analogy is, I think, interesting because it also happens to be a stated reason, right? Security is often a stated reason for a lot of the actions that the government takes. [...]. They have always used it as a cover for these sorts of actions. So, when there are protests happening, there tend to be restrictions on the internet and things like that.

Vikram’s evaluation constructed security as a justifying mechanism for dual-use analogy, reinforcing a securitisation narrative. His example of ‘protests’ and ‘internet restrictions’ framed the first to be seen as the security problem and the latter presented as the solution.

In sum, my respondents expressed concerns about both the lack of effective regulation and excessive control under internet shutdowns in India. While some viewed the existing situation as adequate on both points, others emphasised the need for further development. Together, their perspectives reveal how India’s combined approach of laws and technical operations shapes the governance of online discourse.

8.3.2 United Kingdom

8.3.2.1 Individual Rights in Relation to Shaped Discourse

This subsection reviews three individual rights related to shaped discourse. These are freedom of expression, freedom of thought, conscience and religion, and the right to free election. Through this, this subsection assesses the extent to which the law protects and defines individuals’ capacity to act in the UK.

As discussed in Section 7.3.2.1, Article 10.1 of the Human Rights Act (1998) guarantees freedom of expression, covering the right ‘to receive and impart information and ideas without any interference’. While this definition protects citizens’ freedom of expression from interference, it is a qualified right subject

to restrictions under Article 10.2⁹³. Similarly, Article 9 guarantees ‘freedom of thought, conscience and religion’, reflecting democratic openness to diverse discourses (Human Rights Act, 1998). However, like Article 10, this right is subject to limitations set out in Article 9.2⁹⁴. Together, these provisions demonstrate the UK’s legal consideration of fundamental rights regarding shaped discourse, while their limitations reveal the conditions under which citizens can exercise and preserve them.

The Act also has Article 3, which gives citizens the right to free elections (Human Rights Act, 1998). Unlike Articles 9 and 10, Article 3 is an absolute right in the UK. While this establishes the need to regulate the digital sphere to safeguard electoral integrity, it also protects citizens’ electoral rights and democratic participation in shaping the government.

Although none of these rights - the freedom of expression, freedom of thought, conscience and religion, and the right to free election - relate directly to my shaped discourse theme, they collectively construct a framework for its assessment. Given the existing qualified rights and the state’s need to guarantee free elections, the next subsection investigates existing state working regarding managing shaped discourse in the UK.

8.3.2.2 State Legislation and Regulatory Operations Governing Shaped Discourse

My analysis of FoN data revealed different methods of managing shaped discourse in the UK. I categorise these into two regulatory operations, three DCMS documents, and the Online Safety Act.

The two operations were focused on establishing campaigns and operational units to tackle misinformation and disinformation. The UK government had produced the ‘Don’t Feed the Beast’ campaign and the ‘SHARE’ checklist, ‘Source, Headline, Analyse, Retouched, Error’, to raise public awareness of disinformation and encourage people to engage with accurate information

⁹³ See Human Rights Act, 1998.

⁹⁴ See Human Rights Act, 1998.

(SHARE Checklist, n.d.; UK-FoN, 2021). These campaigns highlight state-wide attempts to increase the public's understanding of the digital sphere. The UK government also established an operative unit during the COVID-19 pandemic, the Cabinet Office's Rapid Response Unit (RRU). In connection to my analysis on -veillance and Section 8.1.2, the RRU not only campaigned and acted against misinformation regarding COVID-19 (GOV.UK, 2020, as cited in UK-FoN, 2021), but also collaborated with the 77th Brigade to monitor related discourse on Twitter (see Carlo *et al.*, 2023, cited in Section 8.1.2). Together, these operations illustrate the UK's structural shaping and adaptation to discourse management during both routine periods and public emergencies.

The Department for Digital, Culture, Media, and Sport (DCMS) published three documents related to shaped discourse in 2019, one of which later became legislation. The first report was 'Disinformation and "fake news": Final Report' (Parliament.uk, 2019, as cited in UK-FoN, 2021). This set out the risks posed by online advertising and political campaigning, concluding that existing 'electoral law [was] not fit for purpose' (Department for Digital Culture, Media, and Sport, 2019, p. 60). This report revealed a structural gap in protecting free elections (see Article 3 of the Human Rights Act above) and exposed a structural vulnerability to online manipulation.

The second report published jointly by the DCMS and Home Office was the 'Online Harms White Paper', through which discussions on 'harmful' content debates such as 'disinformation', 'trolling', and 'hate speech' emerged (Department for Digital, Culture, Media, and Sport, 2019, as cited in UK-FoN, 2021). These not only reflected the discourse shaping operations already discussed in Part 8.1, but also led to the enactment of the Online Safety Act in 2023. This explains the social construction of the Act, which regulates discourse by mandating the removal of illegal content.

The third report, 'Deepfakes and Audio-visual Disinformation', was published by the DCMS Centre for Data Ethics and Innovation (CDEI) (Centre for Data Ethics and Innovation, 2019, as cited in UK-FoN, 2021). It framed manipulated media as having a dual-use character, noting that it could be used by totalitarian regimes

or fanatical groups and had the power to manipulate political discourse and ‘destabilise democracies’ (Citron and Chesney, 2019, as cited in Centre for Data Ethics and Innovation, 2019). This CDEI (2019) report called for increasing public education to tackle misinformation and deepfakes, which links their decision back to the campaigns discussed above.

Unlike previous themes, my findings on shaped discourse show operational methods - such as campaigns and RRU - being used to increase the public’s understanding and to monitor SMP discourse, as well as documentary workings of DMCS and Online Safety Act. While these three reports reflect a serious consideration and evaluation of shaped discourse, they also reveal some inadequacies in enforcement with the exception of the Online White Harm paper which became the Online Safety Act. This exception may suggest that the regulatory problems highlighted in fake news and deepfake reports could be addressed through a similar use of legislation in the future.

8.3.2.3 Legal Concerns about Shaped Discourse

As outlined in Subsection 6.3.2.3, the majority of the public expressed trust in the UK courts and judicial system. This subsection analyses three concerns my respondents raised regarding the legal arrangements for managing shaped discourse. These are about the data protection laws, access to information, and its restriction due to the platforms’ technical features.

First, one of my respondents asserted the inadequacy of data protection laws in the UK when discussing users’ experiences with targeted and manipulated content. According to Tom, the regulations did not cover appropriate use of personal data, where citizens’ data were being used for ‘profiling for electoral purposes [...], political parties here in the UK made with the system in order to target people with political advertisements, and so forth’. He described such uses of personal data as ‘illegal’, comparing the situation in the UK with that in other countries:

[...] a couple of decisions from the general data protection authorities that found the illegality of these systems [...] the US and the EU start to discuss algorithmic accountability as well [...] if we look at the United

Kingdom, the situation is a bit weird, right? Because they are liberal, they're the only country in the world, which is basically watering down data protection, because of the benefits of Brexit and all this sort of [respondent moved to another point without finishing the sentence].

Tom criticised the UK, framing its post-Brexit regulatory developments as inadequate when compared to the EU and the US, which are advancing their algorithmic accountability. His critique can be validated by the UK government's attempts to introduce 'The Data Protection and Digital Information Bill' in 2022, which was dropped in 2023 (see Section 6.3.2 for more detail).

Second, one respondent, Sarah, raised her legal concern about access to information:

So, freedom of information is all about transparency, accountability and scrutiny, and Article 10 is about the right to receive and impart information and ideas, but there's a presumption that you will have access to accurate information or information that allows you to decide whether or not the information you're receiving is accurate. And you then have the other rule of broadcasters to be impartial, although clearly the written word and the TV word is biased.

Sarah's emphasis on 'accurate information' framed the constructed narrative over the right to information as creating expectations of accuracy, even though the law does not define it in these terms. She further explained:

Teachers were saying 'do not rely on Wikipedia as being the source of information'. And therefore, the veracity the provenance of the information that you're using or sourcing is really important, and social media has a lot of opinions in it. And usually, it's about sharing information that's been obtained from other sources. So, it's a bit like a melting pot of information, ideas and opinions. So, it's up to the individual to decide how accurate it is, essentially who they connect with, who they follow, what they retweet or share.

Sarah's point framed the shifting responsibility for verifying accurate information onto individual users rather than awaiting structural changes. This view complements Ofcom's (2023, p.18) findings, which show that only 41% of people try to verify the information they encounter online. Together, these points underscore the importance of improving the public's understanding of

information, as was also outlined in the DCMS report on deepfakes mentioned above.

The third concern was about restricting access to information. Claire asserted ‘the right to information [...] from a variety of viewpoints and different sources’. She emphasised not just access itself, but the ability to draw from multiple sources. Unlike content removal, where a platform removes items based on its own policies or government requests⁹⁵, Claire pointed out restrictions created via content curation:

Which is more about how the platforms are presenting because, even if they don't take down content, they still have ways to make sure that essentially, it doesn't spread right. So, no one gets to see it, which can have the same effect, almost, on people's right to receive information.

Claire's example highlights how platform curation complicates the protection of access to information, creating a grey area for regulatory mechanisms. From her perspective, it not only limits an individual's freedom of expression but also another user's right to receive that information.

Overall, my three respondents expressed distinct legal concerns that together form a triadic assessment of shaped discourse governance in the UK. While Tom criticised the government for its structural inadequacy, Sarah argued that people need to be more responsible in selecting which information they engage with, and Claire highlighted the complexity of platform features in preserving the right to access information. Together, these reflect structuration, agency, and technology-related concerns regarding the governance of shaped discourse in the UK.

⁹⁵ Such as Twitter's content removal in response to legal demands while Facebook removes content based on local law in the user's country, as discussed in Part 7.2.

8.4 Experts' Concerns and Views on the Implications of Shaped Discourse on the Public

8.4.1 India

8.4.1.1 Influence on the Public Discourse

Before analysing my respondents' perceptions on the influence of shaped discourse in the public, I incorporate public opinion data to provide a general contextualisation of trust in public discourse in India. According to Edelman (2022, p.13), a majority of Indians believe that misinformation could be used as a weapon (84%) and that technology may make it harder to distinguish reality from falsehood (75%). While these findings indicate widespread anxiety and distrust, this section analyses my respondents' concerns on disrupted discourse, the influence it has on people's views and opinions, and the public's awareness of shaped discourse in India.

The first concern raised was the disruption of discourse on SMPs. Sanjay assessed this external interference, focusing on its healthiness:

Now, that discourse can be healthy, which is why social media is important. But I have not seen a single sign of a healthy discourse in the last eight years. It's, you know, there are ad hominem attacks all around, they are the only sort of recipe for discourse today.

Sanjay contrasted ideal and 'healthy' discourse with the realities of attacks and hostility he observed in practice. His reference to the 'last eight years' points to a decline in the quality of online discourse. The significance of such disruption is further explained below.

The second concern my respondents raised was shaped discourse's impact on people's perceptions and opinions. One way this was discussed was in terms of its influence on people's views. Amit commented that discourse can '[...] shape any opinion, any image of people [...] and then the larger discourse in politics'. Amit's view emphasised the multi-layered influence of discourse in society. This underscores its power and the extent to which discourse might shape public perceptions and socio-political narratives. The other way a respondent

approached shaped discourse's influence on people's perceptions and opinions was through consensus building and affirming their views on SMPs. According to Nikhil:

Social media plays an extremely significant role within consensus building in politics. And beyond that, social media platforms, particularly WhatsApp, play a very outsized role in information acquisition, so how do citizens acquire or view political information, but this also comes with its own sandbox in terms of consensus building. Because social media platforms allow for micro targeting, as well as targeted propaganda that is built on psychological profiles like marketing profiles, so that social media companies are able to construct on individuals.

Nikhil's reference to 'micro targeting' underscored how users' data are used against them to reinforce their pre-existing beliefs. This suggests a non-organic consensus building through algorithms and psychological profiling by platforms. Similarly, Vikram pointed out that it was 'not just one piece of content, this is a systemised process in the sense that this information is sent out every day'. When both viewpoints are merged, it illustrates a systematic way of affirming not only users' ideas or opinions, but also 'feeds into your confirmation bias of people' (Amit).

The third concern raised was the public's awareness of discourse operations. Some respondents approached this through public awareness and digital literacy. As Karan put it:

Users with a high level of digital literacy, they're able to curate their own experiences and they selectively engage in political content. And then with users who have a lower level of digital literacy, they are usually the folks who are exposed to a significantly more political environment on social media.

Karan's observation distinguished between those with high or low digital literacy, categorising their respective abilities to engage with the SMP context. Like Karan, Amit had a similar categorisation:

[...] people who are aware that's how the content is being shown to them, they are more aware of what they should consume and what they should not. I think many people would hardly use Facebook as much as Twitter or Instagram because there's been so much out there that Facebook has

been manipulative in so many ways. [...] People who know that the information is coming from trustworthy sources, then they would be more keen to reshare, spread it and ignore not coming from those [referring to their ability to ignore inaccurate sources]. So, awareness about how a platform works, what its flaws are, what its good parts are, is definitely helpful in how these platforms are used in the right way.

Amit framed awareness of platform mechanisms and source credibility as protective mechanisms against manipulation. From his account, these resemble the characteristics of people with high digital literacy. Amit then described users with a lower awareness as:

They wouldn't be aware of promoted content. They won't be aware of how the algorithm works. They wouldn't know how trolled algorithms work. So, for them, the impact is just about what they see on their newsfeed.

Amit's view reflected on how a limited understanding of discourse on SMPs makes users with lower digital literacy more vulnerable to shaped discourse. One implication of this is the polarisation it creates among users; it divides them into camps on SMPs. According to Nikhil:

The growing political polarisation based on algorithmically suggested content, which also pushes people towards, for in the case of YouTube it has been researched and clearly shown that it pushes people towards more fringes and extremist views. And also, reinforcing the in- and out-grouping, where you have growing, like a disappearing middle ground in many countries, we can see that there is a strong political hyperpolarisation within the political discourse, and I think that's also in a large part been enabled, not, it's not been created, social media didn't create these problems, but I do believe that they have been exacerbated because of social media.

Thus, Nikhil portrayed platform algorithms as polarising forces that accelerate and amplify existing social problems. His emphasis on the 'disappearing middle ground' reveals how societies are becoming divided into increasingly extreme groups. He further explained this view through the lens of nationalism:

Targeted misinformation triggers strong feelings of nationalism, which then creates pressures on policymakers to take increasingly aggressive diplomatic and political steps, which can also lead to other problems, not only for individuals but also at state levels.

Nikhil's point framed polarisation as a consequence of targeted misinformation. He emphasised that such polarisation not only remains in the digital sphere but also influences offline reality, events, and politics, like his example of policymakers. The FoN reports also document widely-reported incidents in which misinformation was linked to offline harm. These included news reports of 20 people killed following the circulation of a doctored video on WhatsApp in 2018 (The Guardian, 2018, as cited in India-FoN, 2018); accounts of images from the killing of a child in Syria being edited and circulated to warn Indian parents about alleged murderers, which were reportedly misinterpreted in Rainpada, where five men were killed after offering a biscuit to a girl (McLaughlin, 2018, as cited in India-FoN, 2019); and reports of three people being killed in Maharashtra in 2020 after rumours of thieves and kidnappers coming into their village were posted on social media (Goyal, 2020, as cited in India-FoN, 2020). While these incidents are based on reputable reports rather than legal findings, they illustrate broader concerns raised across my data about how misinformation can escalate into serious life-threatening consequences, which underscores the importance of digital literacy and public awareness of how discourse operates on SMPs.

In summary, my respondents raised varying levels of shaped discourse influence in India, ranging from online disruption to reports of offline murder. Although all these effects are serious, the murders resulting from misinformation and disinformation highlight the severity of the situation. This not only underscores the importance of platforms' algorithmic features and their consequences for social polarisation, but also the broader influence of online discourse in offline spaces. The intersection of online and offline worlds confirms how the triadic dynamic between digital technologies, structural governance, and agencies' response plays a significant role in relation to shaped discourse in India.

8.4.1.2 Impact on Activists, Political Opponents, Journalists, and Women

My respondents described a range of groups and individuals who were negatively influenced by shaped discourse-related reasons in India. I categorise them into

three categories: activists and political opposition, journalists, and women. As set out in Subsection 7.4.1.2, the FoN reports from 2017 traced the initial signals of when these groups began to be affected.

First, I identified concerns relating to activists and political opposition of the ruling party. Vikram asserted that, ‘once you express opposition, you are also then exposed to push back [...] abuse, trolling from people who disagree [...] sometimes that could be organic, sometimes it could be organised’. His account illustrates the hostile environment, and the risk opposition faces in online engagement. Giving an example about human rights activists, Tarun stated that:

[...] for example, if you were to speak to a human rights activist and ask them why they don't like using Twitter, one of the things that they would say is the attacks, the spam that they get on anything that they may put up, and that is a place where bots certainly played a very big role [...] so the bots could be from somewhere else. And that will also be completely fine. So, I think it may be as restrictive to new bots as Indians, even if they are virtual Indians behind them, being a part of the discourse they're just, I think a part of the internet, this is a problem that's bigger on Twitter than it is on Facebook and on Instagram.

Tarun's comparison of platforms shows how their ecologies and environments reflect the backlash users experience, especially those with opposing views. These observations highlight both the technical and non-technical reactions users encounter in response to their critical content on SMPs. Another example that further supports this was when India's discourse regulation impacted on opposition and activists. In relation to the internet restrictions imposed during protests, Priya argued:

[...] what happens during protests is that people use the internet to coordinate, right? if three-four people are going for the protest, they will coordinate [...] how they're going to go or is there something in there, in an emergency that's how they coordinate. So, during an internet shutdown, then when you're blocking the means of people from coordinating [...] It surely comes down heavily on mass, especially for minorities, they're not able to participate. [...] So, if you're restricting their manner, like, the things that make them feel safe, how do you suppose that they will be stepping out?

Here Priya underscored how restrictions hinder people from participating in protests by creating difficulties in coordinating and communicating at such

critical times. Together, my respondents' assessments illustrate the political intolerance and the resulting suppression that critical voices experience in India.

Second, two of my journalist respondents, both of whom expressed critical positions on the BJP, highlighted journalists as a distinct profession that was affected by shaped discourse on SMPs. Sanjay explained this through his own experiences and observations, citing harmful and targeted uses of discourse against journalists, including 'threatening phone calls', 'trolling', 'doxing', and 'deepfakes'. This highlights not only the dual-use nature of these operations but also their deliberate weaponisation to target journalists. From a different perspective, Amit expressed the difficulty of spreading accurate information on SMPs:

An individual journalist can never beat an army [referring to political armies] when there is an army to make certain content viral [...] So yes, there is a huge challenge for journalists to reach out to more and more audiences. I mean, no journalist and even small media houses which are actually doing the job, they don't have the resources to put in promotion or place advertisements [...] unless there is a backing from large media houses or corporates to promote that. So yeah, it does skew the space which is available for the right and truthful content to go out.

Amit contrasted the content shared by independent journalists with that of political armies, deeming the size and resources of political armies to be limiting factors for independent journalists. Together, the targeting of journalists (Sanjay) and the struggles they face when spreading their content (Amit) reveal the specific sectoral implications journalists face from SMPs.

Third, some of my respondents viewed women as being distinctly affected on SMPs. Priya explained this by stating that 'they think before posting; women especially they have a hard time because there's a lot of trolling. There's a lot of backlashes they see. People are scared of posting online in case they'll be tracked down. I mean, independent opinions are restricted'. Priya indicated the gender-specific impact faced by women online and suggested how this leads to self-censorship. Similarly, Vikram included women among the groups he thought were influenced by SMPs:

And to some extent social media plays an important role in that and it still gives you a place to do that [referring to expressing opposite opinions]. [...] anyone can have an account, you can also then be exposed when you put out this information, when you express opposition, you're also then exposed to push back, right? Abuse, trolling from people who disagree with you, sometimes that could be organic, sometimes it could be an organised effort to specifically go after especially journalists, especially people from minority communities, especially women. They face a disproportionate respond of push back in those cases for expressing their views.

Vikram's view illustrates the duality of SMPs; while these platforms provide a venue for free expression, the opinions expressed can disproportionately expose abuse and hostility experienced by certain groups.

Overall, the above analysis reflects how shaped discourse affects different sets of individuals through political backlash, targeted operations, difficulties experienced in sharing accurate content, and the need to self-censor due to trolling. While some of my respondents' accounts pointed to real-life implications, as discussed in the previous subsection, they also reflected on the state-level context given in Chapter 3, like freedom issues reported in the Freedom in the World reports. These dynamics reveal not only the state's influence on the digital sphere, but also the effects of digital structuration on the Indian public.

8.4.1.3 Impact on Democracy

My respondents considered democracy one of the implications of shaped discourse on the public. Before discussing their statements, I acknowledge that the public opinion data on trust in democracy and views of the Indian government (Devlin, 2019), discussed in Subsection 6.4.1.2, remains as background context for this subsection. Focusing specifically on shaped discourse, I now analyse my respondents' views on its democratic impact at domestic, international, and theoretical levels.

First, some respondents evaluated the democratic implications of shaped discourse by focusing on domestic politics. Sanjay explained this by examining political leaders' attitudes towards trolls:

You will find that the Prime Minister's Twitter accounts follow some of the most vicious trolls that are on Twitter today. You will see that these are trolls that leave threats, death threats. They have repeatedly spoken about maiming and dismembering and killing journalists, activists, lawyers in the most gruesome ways possible. And they are being followed by the Prime Minister of this country. So, [...] there is a link between the government's elections and the trolling.

Sanjay interpreted the Prime Minister's act of following trolls as an indication of executive support for their behaviour. This observation not only supports the subsection above in terms of how groups were subjected to backlash on SMPs but also highlights the politicised and polarised environment of SMPs in India. This, in turn, raises questions about the executive leadership of the ruling party's online engagement and digital accountability.

Another way my respondents evaluated the democratic implications of shaped discourse was through state elections. Karan argued that SMPs had been shaping public discourse since the 2014 elections:

But it also must be kept in mind that the ability of social media to shape public discourse has really exploded since 2014, so I would say that it's unclear whether it's tied to the specific party or it's a general trend.

The language Karan used constructed the politicisation of SMPs during elections as a broader digital shift rather than attributing it to a specific party. Similar to Karan's point on the unclear origins of these operations, Vikram stated that there was uncertainty about whether they were 'a manipulation from a foreign actor' or 'internal political dissent'. This point raised the possibility of international interference during elections. Either way, both views made it clear that Indian discourse on SMPs had experienced interference during elections, illustrating a challenge observed in the digital sphere.

Second, my respondents discussed external interference in shaped discourse by referring to various global actors. For instance, Ravi, Sanjay, and Manish cited the Cambridge Analytica scandal regarding interference in US and UK elections. This shared view indicated a constructed narrative in which Cambridge Analytica influenced perceptions and shaped thinking in other countries. From different

rationales, Sanjay and Tarun pointed out that other political parties and leaders of democratic countries, including the Conservatives in the UK, Trump in the US, Bolsonaro in Brazil, Erdogan in Turkey, Netanyahu in Israel, and others in the Philippines, Hungary, Belarus, and Russia, had taken undemocratic actions and shaped SMP discourse for political reasons, just like in India. This comparison demonstrated a normalisation and justification of the Indian government's undemocratic actions regarding discourse, since they had happened in other democracies too. This consensus led to a questioning of democracy from theoretical perspectives.

Third, my respondents had different interpretations and assessments of democracy from theoretical perspectives. One way this was assessed was through democracy in action versus the democratic processes states follow. According to Sanjay:

They're all democracies but what we are seeing is that they come to power through ostensibly democratic processes, although it can be argued that some of them have rigged electoral processes as well to attain power. So, and once they are in power, they effectively move to weaken the institution, they effectively move to concentrate power in their hands, and they use technology to do it effectively.

Sanjay's point underscored the strategic narratives among these democracies, especially given that power obtained through a democratic process can be used in undemocratic ways (as discussed in the literature on deficit and hybrid democracies in Section 2.1). Similarly, Nikhil argued:

I think that there's a distinction between institutional democracy [...] the process of democracy. And I would say that the process of democracy might be severely undermined by these emerging trends. However, the institutional nature of democracy remains robust. However, the political discourse of democracies has undoubtedly been negatively adversely affected by the advent of social media platforms.

Nikhil's comment not only made a distinction between 'institutional democracy' and the 'process of democracy', like Sanjay, but also pointed out the common negative impact of SMPs on political discourse. Together, these views highlighted that the extent of social media's impact on democracy differed

between a country's democratic process versus democracy in practice. Nikhil further argued that such practical trends had been adopted from authoritarian countries:

So, the idea of using mass surveillance, of seeding mis- and dis-information, of essentially using social media to subvert people's idea of what their political reality is, something that is learned, that has been adopted from these authoritarian countries and has been implemented in other countries in illiberal democracies first and then maybe eventually in democracies as well.

Here Nikhil framed undemocratic digital practices within democracies as learned behaviours imported from authoritarian regimes. His rationale implied that they are not inherent to democracies. While reinforcing an idealist view of democracies, his view connects back to the literature on the transformative adaptation of digital authoritarian features by states that are not authoritarian (see Section 2.2). From a different perspective, Karan assessed the dual effect of discourse in democracies as:

Discourse that tries to securitise social media regulation has inherent threats to democracy because securitisation is typically very hard to roll back and any sort of application of such tools would have to comply with the standards laid out by the Supreme Court. And that's largely again to the European standard of proportionality, so it would have to be authorised by law. It would have to pursue a legitimate aim, would have to be necessarily the least restrictive measure.

Karan framed the securitisation discourse on SMPs as a process that blurs the line between democracies and authoritarian states. The language he used suggests that the extraordinary measures taken in response to perceived threats create a grey zone of hybridity within democracies.

Overall, my respondents' reflections about democracy at domestic, international, and theoretical levels revealed that India exhibits hybrid or deficit democratic features within its digital governance. While most of my respondents reflected on how politicised the situation was in India, some normalised these dynamics, viewing them as part of a global trend. Taken together, these findings reflect the evolving and context-specific nature of digital governance in India.

8.4.2 United Kingdom

8.4.2.1 Limited Awareness due to the Transparency of Shaped Discourse

My UK respondents thought there was limited awareness among the public regarding discourse shaping operations. I analyse these from two aspects: the uncertainty surrounding the accuracy of information and limited transparency.

First, my respondents raised awareness of being influenced due to the difficulty of identifying misinformation and disinformation. Making references to bots on Twitter, Mark described the situation as:

A mind behind all of this that is always trying to influence you. So, you've got to be able to recognise when something is coming from a bot. And that is really, really difficult. And to recognise that you're being manipulated, you're being influenced, you're being told things that may or not be true or may be half-truths. I think this came to its peak in 2016, or that was the first big peak, with both Brexit and Trump. I think that sensible people voted in ways that were against their interests because they believed enough of what was said or perhaps worse than that, they get to the point where they believe nothing, and that's really scary because that leads to anarchy, that 'I don't believe anything, everybody is a liar'. And then you really disappear into your shell, so I think it's hard and anyone who says it's easy or that they can create laws that fix this is probably being a bit naive.

Mark's reference to bots as the 'mind behind all' framed them as manipulative forces embedded within the platform. Such embeddedness makes it difficult to identify what is true or not. His concerns reflect public anxiety due to the erosion of trust and clarity in information. This aligned with Ofcom's (2023, p.18) findings that 77% of people consider the accuracy of the information they encounter online. Additionally, Mark's emphasis on how people felt deceived by such manipulations aligns with Tom's evaluation that people were confused by the information they came across on SMPs during Brexit (as discussed in Section 8.2.2). These points highlight the growing debates surrounding information and its accuracy in the digital sphere.

Second, some respondents thought that awareness was affected by limited transparency in political campaigning during elections. For instance, Lauren

questioned financial interactions during digital campaigning, ‘where the funding was going and what, where things were coming from, and this is the problem with the social media environment’. Her comment raises two critical points: concerns about parties and the difficulty of tracing political campaigning spending. The first can be supported by data from the Office for National Statistics, which found that 68% of people had either low or no trust in political parties in the UK (ONS, 2024). The latter can be complemented with the Electoral Commission’s (2023) findings, which showed that 58% of people did not believe party funding was transparent and 60% thought there was inadequate regulation of the money political parties spend on campaigns. Lauren further referred to the Brexit and Cambridge Analytica scandal, stating that:

So, I'm talking about the funding of a programme like that Cambridge Analytica programme of data collection and then the targeting of information, but most people would receive that without a clue where it was coming from, and that's the case for most political campaigns really.

Lauren depicted financial spending and economic sources as a limitation on the public’s awareness of political party campaigning during elections. Although her example specifically referred to the Cambridge Analytica scandal, she suggested that this reflects a broader pattern in the UK, complementing the public opinion data from the Electoral Commission (2023) noted above.

Despite approaching it from different lenses, both Mark and Tom’s points about the difficulty of identifying misinformation and disinformation, along with Lauren’s comment on digital campaigning, referred to the Cambridge Analytica scandal. This illustrates the continued effect of the scandal on shaped discourse in the UK. Overall, the above analysis underscores the multi-stakeholder and complex nature of the digital sphere, and exposes an interplay among digital structuration, like platforms’ bots and advertisement features of platforms, governments, political parties, and the public.

8.4.2.2 Impact on Women and Religious Groups

My respondents opined that shaped discourse has different impacts on women and religious groups in the UK than on other users. Their reflections align with FoN reports from 2016 to 2021, which consistently highlighted the targeting of women online (UK-FoN, 2016-2021).

First, some respondents noted that discourse on SMPs was gendered. As Claire put it, one of the reasons behind this was the controversy about how to define a woman:

At the moment we think it's controversial to say, 'What is a woman?' That's a controversial topic these days. Ten years ago, you wouldn't think that is a controversial topic, today it is a political topic.

Claire's observation highlighted a societal transformation regarding gender, framing such change as it becoming difficult to even define what a woman is. From her personal research experiences and observations, Lauren pondered how trolling affects women and marginalised groups online:

I think it [trolling] was felt for some people it was almost defined essentially as abuse, as kind of toxic, as abusive, as preying on marginalised groups, and incredibly damaging in that sense. But other groups we did had a sense it was just people being playful, it didn't really make much difference, it doesn't create anxiety, it was something that they even engaged in themselves. But I do think, [...] if you take, say, female journalists, female politicians get an awful lot of trolling and quite horrible abuse about their appearance and things that I don't think men get. And even though some people might see that as playful, if you are on the receiving end of that I can tell you it's not playful [...] And actually so you just silence people in that respect, and we had a lot of users who basically said 'I just can't handle it, I remove myself, I never say anything controversial' [...] it plays a structural role in silencing people I think, particularly women, marginalised groups, I'm sure you know ethnicity plays a role as well for sure and it's very, very difficult.

Lauren's description that trolling and abuse against women is 'not playful' exposes how some people perceive such actions as trivial and inconsequential. Instead, she framed them as having a 'silencing' effect, which complements the self-censorship discussions made in relation to content control (Section 7.4.2). While Lauren approached this from the perspective of women's experiences, her

observation reflects a broader public view about online hostility. According to Ofcom's (2023, p.12) survey findings, 92% of people believe that some individuals act in a 'cruel or unkind' way towards others on certain platforms. This suggests that while the issue she raised might be significant for women, it is a widely recognised problem across platforms.

Second, insights from my respondent David, together with data from FoN reports, reflected on the specific impact experienced by religious minorities in the UK. David commented on accusations towards Evangelical Christians:

But the problem comes when you examine how people use the word 'extremist'. I mean, an extremist is basically somebody who is to the right of me or to the left of me, that's the danger of the label 'extremism', is it just means somebody with views in a very different from my own on either end of the political spectrum. And again, as an Evangelical Christian, I know that we do get accused by some people of being extremists, a nice mild-mannered middle class vicar that I can think of, who was labelled an extremist by somebody who just was just trying to marginalise his opinion [...]. I think that certain points of view are disfavoured and downgraded and I think it's inevitable even if you're kind of a relatively fair-minded person programming an algorithm, but if you have a particular view of the world that comes through in the way you write your code.

David's reflections challenged the neutrality of the label 'extremism', framing it as a subjective and politically charged term used to marginalise minority views, which he experienced as an Evangelical Christian. His critique extended to algorithms and suggested that regardless of how 'fair-minded' a programmer might be their worldview would inevitably shape their code. Similarly, FoN reports shared a study conducted by advocacy group Hope Not Hate, which found that some activists were using terrorist incidents in the UK to feed anti-Muslim views on SMPs (Hope Not Hate, as cited in UK-FoN, 2020). These findings illustrate negative experiences of those who belong to religious minority groups and how they are influenced in the UK.

In sum, the above analysis highlights how women and religious minorities were specifically affected by shaped discourse in the UK. Unlike the country's representative, inclusive, and equal context portrayed in Chapter 3, my research analysis shows some negative experiences online. This suggests a weaker

democratic environment in the digital sphere of the UK than in its state-level structures.

8.4.2.3 (Dis)Trust of Shaped Discourse

The final discussion arose from my respondents' insights on trust. I categorise these into three areas for analysis: SMPs, the government, and democracy.

First, my respondents raised various rationales behind the public's lack of trust in SMPs. Some attributed this distrust to uncertainties surrounding platforms. Focusing on Facebook, Lauren stated that 'we learnt Facebook's capability to use our data to tailor our behaviour', and Anna commented that 'we don't know about how Facebook is used for political advertising'. Despite revelations about the platform's use of personal data and targeted advertisements during the Cambridge Analytica scandal, both respondents suggested persistent uncertainties had led to their distrust in the platform. This aligns with a cybersecurity company's finding that only 20% of users trust advertisements on Facebook in the UK (Menlo Security, 2023). Such distrust of online advertisements appears to extend broadly, as reflected in Ofcom's (2023, p.24) survey showing that 91% of internet users have managed advertisement settings on the platform they use. This illustrates a reflexive monitoring, as one of my respondents, Mark, described his platform choices:

The most dangerous place to put your data [referring to Facebook], because we know in the past, they have happily resold information to people that has been used, in these cases to manipulate a whole population to vote in a particular way. And that's why I don't use Facebook. I felt Twitter was different. Maybe I need to finally get onto Mastodon and come off Twitter because I'm not sure I could trust Elon Musk either.

While Mark thought that Facebook had been a threat for a long time due to data selling and political manipulation, the language he used revealed a trust shift in Twitter following its acquisition by Elon Musk. Both findings from Ofcom and Mark point to a pattern of reflexive monitoring that is grounded in agency, illustrating how individuals critically assess their actions online. Similarly, Lauren shared from personal observations that:

Twitter has obviously had a complete redesign in recent weeks and it seems so algorithmically driven now [...] And what I've found increasingly is, rather than the sort of information environment that individuals have set up which is tailored to their interests, their preferences, it's absolutely driven by past behaviour, not only of themselves but other people who might be categorised as like them. And so actually I think our social media environments are probably becoming more similar. [...] I'm seeing content which is related to the most controversial discussion that's going on in the country more generally. [...] I'm not seeing those professional tweets from people I know or work within academia because they're not controversial enough, they're actually just promoting decent work, we're talking about making very useful comments on other things, possibly about academic works.

Like Mark, Lauren had observed a change in Twitter, noting that the platform shows content related to 'controversial discussion' in the country. This suggests noticing a change in the platform's algorithms and highlights how it limits users' engagement. Together, my respondents, alongside public opinion data, expressed distrust in platforms based on how they interpreted and constructed platform technologies and actions, like political advertisements, data-selling practices, and algorithmic changes.

Second, some respondents expressed distrust in the UK government, providing primary insights that complemented the data about low levels of public trust in the government (see Subsection 6.4.2.2) and its responsible regulation of new technologies (see Subsection 6.2.2.2). Emily evaluated this by focusing on political campaigning methods:

[...] so I think I trust traditional methods more because there was more accountability for me to see what happened, like who paid for this leaflet and who paid for a certain advertisement in the UK [...] but it [referring to digital campaigns] feels much less up-front now, so I think I would be more suspicious of an advert [...] I wouldn't be so quick to believe what it says. And I also feel like there's less trust in me, and that feels then I want to have less trust, like that, then it feels like it has to go both ways. I feel like the desire to monitor every action and keep track of it and to do that without really good consent on every part.

Emily distinguished trust between traditional and digital methods of political campaigning, framing the former as more trustworthy and authentic than the latter. From a different perspective, Mark expressed his distrust by criticising

those who had not taken adequate measures after the Cambridge Analytica scandal to prevent the same thing from happening again:

We don't seem to be adult enough to say, 'this is so important that it could happen again'. And because it can happen again, and it might be even more serious next time, we really need to understand why it happened and try to stop it from happening some more. It seems as if the UK doesn't want to look. And partly of course it doesn't want to look because the politicians in power now are some of those who were happy to reap the benefits as they saw it of this illegal activity.

Mark's account conveyed distrust and disappointment in the government's failure to take precautionary measures and to prevent user manipulation during elections. His remarks that 'it seems as if the UK doesn't want to look' and that 'some of those who are happy to reap the benefits' portrayed certain political actors as being beneficiaries of such manipulation, framing their inaction as a calculated choice. Unlike Mark's stymied expectations for a change, Lauren expressed no doubt about the UK government's interference in SMPs:

[...] I know the UK government does it as well, they do actually lobby social media platforms [...]. We don't really know the extent of it, but we do know that there's a lot of that discussion between the owners of platforms and state governments and there's no question UK is involved in this kind of informal censorship and of course through the different terrorist kind of monitoring and so on and so forth. I think there's a lot more going on that we don't really know about, and the level of data actually collected by governments itself is, again, it's unknown. [...] I don't know evidence but I don't doubt the UK state gets involved in interfering in foreign social media environments as well as the US state does when it comes to, say, discussion of Israel-Palestine and trying to get Hezbollah terrorist groups as they see them banned from Facebook and all the rest of it, the kinds of work that they do.

Lauren's assertion of certainty, despite limited evidence, revealed a discourse that was critical of institutional transparency. Her likening of the UK with the US in influencing online narratives positioned democratic states within the same spectrum of manipulative behaviour that is often attributed to authoritarian regimes. While Emily and Mark focused on the UK's digital governance during elections, Lauren offered a broader assessment of both national and international interference. Taken together, these views reflect multi-level insights into distrust surrounding digital governance in the UK.

Third, my respondents assessed public trust by reflecting on democracy. This echoed the public opinion data regarding only 33% democratic satisfaction cited in Subsection 6.4.2.2 (Electoral Commission, 2023). Emily argued that democracy in theory differed to how it was practiced in the UK:

[...] wherever democratic theory is, one that's about what's positive or what's in reality, because some of the theory's about trying to capture what's there and some of it's about saying what it should be. And I'm really interested to see what you answered the writing on this, because I often stay away from the word 'democracy' and I try to just talk about political participation in general, because it's such a difficult word. And I think transparency and accountability and the freedom for people to feel the ability to understand and express themselves. And there's trust, trust between different entities. All of those things are ways I define democracy, words I would use in the sentence about democracy. And in comparison, to that definition of my theory of democracy and then what's in practice, I think there's very little transparency and accountability. And I think there's very little trust [...].

Acknowledging different theories of democracy, Emily had developed her own definition using terms such as 'political participation', 'transparency', 'accountability', 'freedom', and 'trust'. Despite her initial hesitation to comment on democracy, Emily's comparison between this definition and actual circumstances led her to make a critical assessment of its practice. From a different rationale, Lauren argued that elections were not inherently democratic:

I don't think any election's democratic because propaganda, mainstream media represent the elites in this country, and they always have and that's the information we receive. It's also true that individuals are capable of independent thought. They look at media, it is incredibly influential, but they do other things in their life, they have some of their own experience, they can apply logic and reasoning, they can go and talk to other people, which we always do. Who do we talk to? Our family or children or partners or parents, and we talk to other people in a university, classroom. We talk to other people in the workplace. So even though I'm saying social media is an extension of all of those and has become increasingly important, [...] information is very, very targeted and very powerful and steering our decision making. So yes, it's undemocratic if these groups are - without any transparency, without any kind of notice of funding - they're stealing data. That's legally wrong, and I think as well as morally wrong, and is really challenging in terms of democratic functioning.

Lauren's account emphasised both organic and inorganic activities that influence individual thought, framing the latter as a challenge to democracies. She explained that these further contribute to democratic distrust:

I think the government were doing a good job of eroding trust all on its own, actually [...] but there's no question that social media moved into the space left and probably exacerbated the problems with trust in the public sphere to the point where many people don't know who to trust, what to trust, whether they trust anything at all. Actually, that's not a good position for a democracy to be in, because democracy is founded on some sense of trust in the system. And if it doesn't have that it's a real problem, because people are not getting involved in politics, and by that I mean even at the lowest level of voting, or disengaged from what goes on, or not investing in the kind of mechanisms that we have to uphold democracy, and they don't trust the experts who speak, and that's a real problem.

Lauren's interpretation framed digital interference that shapes individual opinion as a form of restriction on fundamental democratic participation, such as voting. From a more international point, Jessica commented on distrust in terms of non-democratic actions:

I think it's different shades of non-democracy in different places. But I think that democracy's in a crisis across the world and we're seeing that a lot of the mechanisms that democracy have developed are just not applicable when it comes to digital services and data platforms, because the tools that we have that are meant for us, to kind of guard us, are just not appropriate for what is happening at the moment. So, I think that a lot of democracies need to look inside themselves and see how they need to change in order to provide the appropriate protection mechanisms and rights for people in order for them to actually be useful and effective.

Jessica's view highlighted that the form of a state's governance does not guarantee the nature of its digital governance. She argued that the use of digital tools and operations may not always be 'appropriate', reflecting on their dual-use character⁹⁶. In contrast to previous respondents' contemporary assessments of democracy, Anna asserted that:

⁹⁶ See the Introduction of this chapter and Chapter 1 for the concept of 'dual-use'.

[...] democracy is not a product but a process. It's something you have to constantly review and fight for. And I think we had a nice time for a couple of decades, but the fight is back on us now.

Anna's account reminds us that democracy is not an end in itself but a process that has evolved and been adapted over time (as also discussed in the literature; see Section 2.1). Thus, rather than framing the current situation as a failure, Anna's narrative highlights the need to repair and strengthen democracy.

In summary, the above analysis demonstrates my respondents' multi-layered understanding of distrust toward SMPs, the UK government, and democracy. The findings reveal that manipulation and targeting as embedded within structural arrangements and amplified by technological systems, were argued to be shaping individual thought and practice. This not only underscores the interplay of the structuration framework but also highlights the mixed nature of digital governance in the UK, where democratic ideals coexist with non-democratic practices.

8.5 Conclusion

Shaped discourse is my last research theme through which I have analysed the digital governance of SMPs in India and UK. The analysis presented in this chapter can be summarised in six points.

First, both countries had discourse shaping operations conducted by various actors during politically sensitive times, like the 2019 elections and the COVID-19 pandemic. In India, party-affiliated political armies carried out extensive operations online, whereas in the UK, political parties were linked with different disinformation operations such as doctored videos and amplifying posts by small groups like Momentum. Both countries also had debates about involving private companies in their data-driven political campaigning, where they had the Cambridge Analytica firm in common. Distinctively, India had a case where the prime minister's own app was used to spread propaganda, while the UK had a unique case involving a military team monitoring political discourse regarding the Conservative Party's COVID management on Twitter. Together, these findings illustrate how shaped discourse operations can be socio-politically

interpreted by different actors in both countries. This reveals the diversity among stakeholders involved and highlights various technical and non-technical methods employed within their respective national contexts.

Second, both countries interfered with and were interfered by the discourse operations of other countries. India was interfered with by Pakistani political armies and interfered in the UK during the 2019 elections. In contrast, the UK was interfered with by OFBJP-UK and had international operations like targeting terror groups (which were also conducted domestically). This underscores the transnational nature of the digital sphere (as discussed in Chapters 1 and 2) and illustrates how discourse operations can become a strategic dual-use operation for countries.

Third, my respondents set out their perception that SMPs had power over traditional media in terms of their social transformation in becoming a channel of information acquisition and shaping discourse. They highlighted advertisements and inauthentic behaviour on Facebook, as well as bots, trends, and users' capacity to reach great audiences on Twitter as key shaped discourse-related features of the two platforms. These observations showed how integral platform features enabled ways to shape users' discourse. The case of India illustrated the importance of government-SMP relationships, like the differences between Facebook and Twitter. In the UK, my respondents viewed SMP-government relations from broader perspectives and referred directly to only one incident that showed SMP-government engagement: Mark Zuckerberg's refusal to attend UK parliamentary questioning on the Cambridge Analytica scandal. This is not to suggest that one government was stronger than the other but demonstrates different types of engagement and relationships between governments and platforms in both countries' digital governance. Taken together, all of this reveals how the digital governance of SMPs is uniquely constructed in each context through the interaction of structure, agency, and technology.

Fourth, unlike my -veillance and control themes, I found that shaped discourse does not have explicitly connected individual rights that focus on protecting

people and defining their capacity to act, either in the UDHR or in domestic legislation. Instead, I drew on the freedom of thought, freedom of speech, and the right to free elections to address its relevance in the existing legislation. While both countries recognise the freedom of thought and speech as qualified rights that might be limited, the right to free elections was an absolute right in the UK but was not guaranteed in India. These findings illustrate how societal transformation generates new global needs to protect people from shaped discourse, such as the right to accurate information, and indicates a structural gap that constrains people's protection and their capacity to act, as seen in the two countries' differing contexts.

Fifth, unlike my previous themes, I found that both countries had regulatory operations alongside their legal frameworks in relation to shaped discourse. Regulatory operations involved internet shutdowns in India and campaigns and a development of a Rapid Response Unit in the UK. Considering that these operations were conducted at times of protest, public emergencies, or the COVID pandemic, illustrates how both countries operationalised their legal structure to manage discourse. Nevertheless, my analysis revealed persistent issues regarding controlling and regulating shaped discourse. In India, my respondents raised concerns over the politicised implementation of existing laws and highlighted a regulatory gap in controlling discourse, with some warning that such regulation could further proliferate politicisation risks. In contrast, my UK respondents criticised inadequacies in data regulation, problems they had observed with the Online Safety Bill, and discussed the application of freedom of information by distinguishing it from accurate information. Taken together, my respondents' concerns outlined both countries' digital discourse management and the influence this creates on individual rights. In line with the previous point, these findings illustrate an emerging regulatory gap in which states have begun recognising the significance of discourse and are working toward adapting their structural mechanisms.

Sixth, my interviews raised three distinct areas where impact from shaped discourse was most strongly felt in their respective countries. In relation to the public in general, my Indian respondents articulated on the disruption of

discourse online, while my UK respondents stressed on the limited public awareness. They also described specific groups and people that were specifically negatively affected by shaped discourse activities. These include activists, journalists, women, and religious groups in India, and women and religious individuals in the UK. The other impact observed was regarding trust. My Indian respondents addressed trust from democratic debates, giving domestic and international examples. In the UK, respondents considered trust more comprehensively, focusing on SMPs, the government, and democracy. Together, these findings provide insights about the complex interplay of structure, technology, and agency from public perspectives in India and the UK.

This chapter has presented the findings on the final theme of my research. The empirical findings on the socio-political context of operations, the role of SMPs, legal frameworks, and observed implications on the public offer thematic insights for understanding digital governance in both countries. These findings further complement my digital structuration framework, as demonstrated by the different instances of structural, technological, and agential primacy described across the analysis. The next chapter comprises a thorough discussion of all my research findings set out in Chapters 6 to 8.

Chapter 9 Discussion

This chapter compares and contrasts India and the UK's digital governance of SMPs based on the findings presented in Chapters 6 to 8, to address my research questions. As detailed in Chapters 1 and 5, this study was guided by three sets of sub-research questions (SRQs) to help answer my main research questions:

Main research questions: How do India and the UK construct their digital governance in relation to social media platforms? What is the broader significance of this for democracies and digital governance?

SRQ.1 What are the existing digital dual-use operations involving social media platforms in India and the UK? Who conducts these operations?

SRQ.2 How do legal frameworks inform the regulation of digital dual-use operations and stakeholders? What legal concerns are raised regarding the digital governance of social media platforms?

SRQ.3 What implications and concerns do experts raise regarding the digital governance of social media platforms and their impact on the public in India and the UK?

To facilitate a detailed discussion, this chapter is divided into four parts. The first three parts focus on my three SRQs: Part 9.1 addresses SRQ.1, Part 9.2 focuses on SRQ.2 and Part 9.3 on SRQ.3. Each of these three parts present comparative discussions of -veillance, content control, and shaped discourse in separate sections. They conclude with a summary section that synthesises my thematic findings to answer each SRQ. The fourth part answers my main research questions by generating digital governance structures and discussing India and the UK's political regimes and digital governance of SMPs.

9.1 Digital Dual-use Operations Involving Social Media Platforms in India and the UK

9.1.1 -Veillance

Drawing on the definition of -veillance and its dual-use nature provided in Chapter 6, this section compares India and the UK's -veillance operations involving SMPs. Based on the summary provided in Table 9.1, I discuss

commonalities⁹⁷ and differences between India and the UK in two subsections below.

Table 9.1: Summary of -veillance operations		
	India	United Kingdom
Government-linked operations		
Dataveillance through regulation	• ID verification • Data retention	• GCHQ • Age verification
Technical -veillance	• NATGRID • CMS • NETRA	• SOCMINT • Test and Trace
Non-technical -veillance	• Lateral -veillance	• 77th Brigade
Government collaborations with external actors		
Government funding	• AASMA	
Tools that were developed by others	• Pegasus	• HateLab Dashboard
International collaboration	• Five Eyes	• Five Eyes
Social Media Platforms	• Facebook • Twitter	• Facebook • Twitter

9.1.1.1 Government-linked Operations

This subsection compares and contrasts three commonalities of -veillance operations in India and the UK.

The first commonality is dataveillance that results from the countries' established regulations. This was seen in ID verification and data retention in India, and in bulk operations and the requirement for ISPs to verify users' ages in the UK. While India's operations highlight targeting data operations on domestic organisations by the central government and judiciary, the operations identified in the UK illustrate a de-centralised format where either a distinct authority conducts the operation (like GCHQ) or it gets diversified under ISPs. One evident difference between the two countries is that, unlike India's domestically focused operations, the UK's operation under GCHQ involves data collection from both domestic and international sources. Despite this difference, both countries signal democratically concerning links, as ascertained from the literature. My

⁹⁷ I have not called them 'similarities' because both countries had approaches in common, but these were unique in their type and context. The same applies to the rest of this chapter.

findings on India's dataveillance through regulation resemble the digital authoritarian example of Russia's data regulations (see Subsection 2.2.1). In the UK, my research findings on GCHQ complement the Snowden revelations and reflect on the changes observed in digital democracies (see Subsection 2.1.1). Together, these points highlight democratic states' proximity to non-democratic digital governance features, while underscoring the dual usability of regulations.

The second commonality is technical -veillance operations. My analysis shows that both the three operations in India - NATGRID, CMS, and NETRA - and the UK's Test and Trace were linked to public emergencies. This came to light following Arjun's reflection about the implications of the 2008 Mumbai attack in India and the COVID-19 pandemic in my analysis of annual FoN reports in the UK. Additionally, the UK also has a SOCMINT operation conducted by the police and local authorities. These operations confirm how both countries have integrated large-scale programmes into their governance.

The third commonality is non-technical -veillance operations. I identified lateral -veillance undertaken by the Cyber Crime Volunteers Programme in India, and Twitter surveillance by the 77th Brigade in the UK. India's programme comprised individual volunteers who monitored SMPs and flagged up content they deemed illegal to the police (see The Economic Times, 2021, and Ministry of Home Affairs, as cited in India-FoN, 2021 in Subsection 6.1.1.1). This de-centralised approach was criticised for a lack of transparency by a respondent, Vikram. In contrast, the UK's non-technical -veillance was centralised, involving the 77th Brigade's monitoring of Twitter during the COVID-19 pandemic (see Carlo *et al.*, 2023 in Subsection 6.1.1.2). This militarised surveillance demonstrated political underpinnings, as it included targeted monitoring to understand how people viewed the Conservative Party's handling of the COVID-19 pandemic, according to the whistle-blower cited in the Big Brother Watch report (see Carlo *et al.*, 2023, p. 64 in Subsection 6.1.1.2). This difference between the two countries' use of civilian versus military personnel not only underscores the dual usability of these operations but also contextualise the digital governance strategy they have adopted. Despite these differences, both countries show similarities in how states adopt digital technologies to consolidate control, as discussed in the

digital authoritarian literature. While India's programme resembles China's '50-Centers' (Diamond, 2010; Bulovsky, 2019) and Iran's Revolutionary Guards (Centre for Human Rights in Iran, 2015, as cited in Michaelsen, 2017, p. 467), the UK's monitoring of Twitter for political discourse indicates a regime-focused operation, like digital authoritarianism (see Subsection 2.2.1 for the literature review).

Overall, my findings on digital dual-use operations underscore interpretations and integration of -veillance operations in the context of India and the UK. These operations highlighted not only the regular and crisis management of how both countries used technology in their governance but also confirmed their centrality to the respective governments. One key difference between the two is that, unlike India involving civilians in its government programme, the UK's -veillance operations include police and military forces. Taken together, these findings show links to the regime-focused actions and operations described in the digital authoritarian literature, and they also reflect broader concerns about the weakening of democratic accountability in states' digital practices. Nonetheless, government-linked operations are just one part of the discussion; the next subsection focuses on government collaborations with external actors.

9.1.1.2 Government Collaborations with External Actors

My research identified three commonalities between the Indian and UK governments' collaborations with external actors regarding their -veillance operations.

The first commonality is the governments' use of -veillance tools that have been developed externally. In India, this involved the government's funding for the Advanced Application for Social Media Analytics (AASMA) and accusations about its use of Pegasus spyware (see India-FoN, 2019-21 in Subsection 6.1.1.2). Both these operations illustrate uncertainty as they are indirectly linked to the government, affecting their traceability. In contrast, the Cardiff University's HateLab project, which is an SMP content monitoring tool, has been adopted by the National Online Hate Crime Hub and the Welsh government to tackle hate speech (see Osborne, 2023 in Subsection 6.1.2.2). Unlike India's reported

procurement of Pegasus spyware from an Israeli-linked group, the HateLab project has developed into an international dual-use product adopted by private companies and other governments (see Osborne, 2023 in Subsection 6.1.2.2). Together, these findings exemplify governments' engagement with different actors and contextualises the international market on purchasing and selling dual-use products within their respective countries (see the literature on dual-use technology by Polyakova and Meserole, 2019, and Howells and Henry, 2021 in Subsection 2.2.1).

The second commonality is India and the UK's collaboration with other states in opposing encryption and privacy on Facebook. Both collaborated in writing an open letter that criticised the platform, along with other Five Eyes members and Japan in 2020 (see India-FoN, 2021 and UK-FoN, 2021 in Part 6.1). Such a collaboration among democratic countries reveals their preference for accessing citizens' data, rather than prioritising protecting their right to privacy. This highlights a shift in democratic countries' stance for democratic principles on the digital sphere.

The third commonality is the governments' request to obtain users' data from SMPs, which I analysed through transparency reports and my respondents' assessments. Table 9.2 summarises my analysis of governments' user data requests. It shows that, firstly, Facebook received more government requests than Twitter in both countries. Secondly, although Facebook had a higher compliance rate in the UK, it provided more total data to the Indian government due to its higher number of requests. This case was different for Twitter. Although India made more requests to Twitter than the UK, the platform shared a higher number of user data with the UK due to its higher compliance rate. This underscores the SMPs' role in providing data to the governments, as well as their agency power to decide whether to fulfil these requests.

Table 9.2: Summary of data/information requests from Facebook and Twitter (2019-2021)		
	India	United Kingdom
Facebook		
Government requests	220,899	56,605

Accounts specified	342,993	68,736
Compliance	54% (average)	88.5% (average)
Total number of data provided by Facebook	188,995	60,815
Twitter		
Requests	11,877	2,974
Users specified	33,976	4,067
Compliance	2.6% (average)	46.9% (average)
Total number of data provided by Twitter	829	1,924

My respondents assessed the role of SMPs by highlighting the power they have over data and reflecting on governments' reliance on platforms to obtain data. Regarding the first point, one Indian respondent emphasised SMPs' power through people's dependency on the information shared by platform reporting due to a lack of a comprehensive dataset available in the country (see Karan in Subsection 6.2.1.2). In contrast, a UK respondent interpreted SMPs' power over user data as a form of payment for using 'free' platforms (see Richard in Subsection 6.2.2.2). These perspectives complement the literature on the political economy of social media platforms (see Fuchs, 2024 and Andrejevic, 2011 in Subsection 1.2.2), reflecting how the framing of 'free' services obscures the extraction of user data and labour as SMP profit.

In relation to governments' reliance on SMPs, my respondents expressed doubts about their government's secretive collaborations with them. Two India respondents, alongside a secondary source validation, referred to the government's interference in Twitter (see Nikhil and Vikram and The Wire Staff, 2022 in Subsection 6.1.1.2). In the UK, my respondents shared an unevidenced view about covert government-SMP deals, suggesting that such relationships may weaken effective regulation, enable platforms to blackmail governments, and create risks of user rights being infringed in ways associated with digital authoritarianism (see Jessica and Richard in Subsection 6.2.2.2). Regulatory concerns (raised by Jessica) align with the wider public perception, where only 34% consider the government to responsibly regulate emerging technologies (see ONS, 2024 in Subsection 6.2.2.2). Together, these opinions echo the literature on big technology companies' proximity to political processes (see Kreiss and

McGregor, 2017 in Subsection 1.2.1), supplementing respondents' concerns that government-SMP relations may blur regulatory boundaries, reduce transparency, and risk politicising digital governance.

Overall, my findings on the governments' collaboration outlines their engagement with different stakeholders in their respective contexts and supports the literature's consensus on the multiple-stakeholder character of internet governance (see Flyverbom *et al.*, 2019 in Chapter 2). By examining both the operations integrated within the government and engagements across stakeholders, this section has detailed digital dual-use operations associated with -veillance in the two countries. These findings further provide insights about digital structuration by revealing how -veillance technology has been adopted by states structures and multi-stakeholder agencies within the digital governance systems of India and the UK.

9.1.2 Content Control

Building on my findings presented in Chapter 7, this section compares content control operations in India and the UK. Given the summary depicted in Table 9.3, I compare my findings through four commonalities and then highlight differences between the two countries.

Table 9.3: Summary of content control operations		
	India	United Kingdom
Topics	• Long list	• Short list: copyright infringement, promotion of terrorism, and depictions of child sexual abuse
Ways of removing content	• Direct: Department of Telecommunications, government orders, court orders, the Election Commission, and the law, Cyber Crime Volunteers Programme, SMPs • Indirect: pressuring SMPs, technical filtering operations	• IWF • Service providers • CTIRU • Law • SMPs

The first commonality is that both countries maintain lists of topics that they control online. My analysis of the FoN data identified a broad range of controlled topics in India, including socio-political and religious content (see Section 7.1.1), whereas in the UK the controls were centred on three main categories: terror, copyright, and child sexual abuse. India's comprehensive approach reflects the influence of its state-level social and political context in shaping the scope of content control (see Section 3.3). This detailed approach towards content control resembles restrictions set out in Russia's 'Blogger Law' and Iran's development of a 'Halal Internet' (see Subsection 2.2.1). Despite having distinct categories, the UK operations were deemed to be interlinked at certain operational points, like BT's Cleanfeed (see Section 7.1.2). This example showed how the explicit scope of each category was dissolved and intersected in practice.

The second commonality is the use of filtering tools. These were seen in forms of direct and indirect operations in India and centralised and de-centralised operations in the UK. India's direct tools legally required intermediaries to employ automated filtering (see the IT Rules, 2021⁹⁸), and the indirect ones involved purchasing and using filtering tools from private firms (like SNI filtering or Netsweeper in Section 7.1.1). The UK's centralised filtering involved legally mandated tools (see the Online Safety Act in Sections 7.1.2 and 7.3.2) but also the development of such tools in collaboration with authorities, like the software developed by the Home Office and ASI Data Science (see Home Office, 2018; Greenfield, 2018, as cited in UK-FoN, 2021). The UK's de-centralised operations entailed ISPs developing and using automated content filtering tools, as long as they fit the ISPs' own terms and conditions⁹⁹. Despite different classifications of these operations, both cases illustrate varying levels of connections to the government and underscore the diversity of operations within their contexts.

⁹⁸ Section 4.4 of the IT Rules, 2021 (see Section 7.1.1 and Subsection 7.3.1.2).

⁹⁹ S. 104 of the Digital Economy Act, 2017 (see Section 7.1.2 and Subsection 7.3.2.2).

The third commonality my research discerned is content removals from SMPs, which I compared through platforms' transparency reports and my respondents' assessments. As discussed in Chapter 7, Facebook removes content under local law, while Twitter processes them on a case-by-case basis. This difference between the platforms highlights the importance of their organisational structure and procedures followed in managing content. After addressing this significant insight, I move on to my analysis of SMPs' transparency reports.

Table 9.4 summarises my analysis of Facebook and Twitter's transparency reports between 2019 and 2021. It shows that the UK had more content restricted on Facebook than India, while more content was removed from Twitter in India, despite the UK's higher compliance rate. These findings emphasise the role of SMPs and the law in India and the UK. While informing us about their content controls, these findings also highlight the numerical difference between the platforms' reports on government data requests and content removal. When compared, both countries' total number of SMP requests were lower in terms of content removal than users' data (see Table 9.2 in Subsection 9.1.1.2). This means that India and the UK collected more user data (182,563¹⁰⁰) than removed content (38,546¹⁰¹) from Facebook and Twitter in the years studied in this thesis. Additionally, transparency reports on data requests and content removal show that Facebook complied with government requests more than Twitter in the two countries.

Table 9.4: Summary of content removals from Facebook and Twitter (2019-2021)		
	India	United Kingdom
Facebook		
Total number of contents restricted based on local law	4,751	22,672
Restricted products (high-low)	Posts (3,152) Pages and groups (446) Profiles (288) Comments (1)	Posts (2,787) Pages and groups (270) Comments (24) Profiles (15) Albums (12) Events (11)
Twitter		

¹⁰⁰ Total compliance number data collected from Facebook and Twitter in India and the UK.

¹⁰¹ Total number of contents removed from Facebook and Twitter in India and the UK.

Legal demands	19,924	255
Accounts specified	72,687	501
Compliance (average of 5 reports)	18.2%	32.9%
Total content removed by Twitter	10,989	134.8

Regarding SMPs' role in content control, I have compared my respondents' reflections based on their respective countries. Although Twitter removed more content than Facebook in India, my respondents emphasised the government's closer relationship with Facebook and characterised Twitter as adopting a more resistant stance toward the government (see Ravi and Vikram; Singh and Conger, 2022 in Subsection 7.2.1.2). This contradiction between quantitative data and my respondents' perceptions reveals how narratives about the two platforms are constructed in the country. Additionally, they highlight the value of the large Indian market, which requires SMPs to maintain a good relationship with the government (see Ravi and Vikram in Subsection 7.2.1.2). In comparison, my UK respondents deemed their government's relationship with SMPs as a form of cooperation, alluding to the government's interest in accessing and controlling SMPs (see Richard and Anna in Subsection 7.2.2.2). One respondent interpreted this as negatively influencing the objective regulation of SMPs (see Jessica in Subsection 7.2.2.2), aligning with public opinion data showing that only 34% of adults believe the government is responsibly regulating emerging technologies (see ONS, 2024 in Subsection 7.2.2.2). Others, however, highlighted the political power of the UK and the resulting need for SMPs to align with government interests (see Tom and Lauren in Subsection 7.2.2.2). Despite their different perspectives, respondents from both countries agreed that SMPs must maintain positive relations with governments. This informative perspective illustrates an interdependent relationship that is affected by the economic value of SMPs, reflecting the literature discussed in Chapter 1 (such as Fuchs, 2024, and Andrejevic, 2011 in Subsection 1.2.2), and highlights how market incentives operate as a form of control within government-SMP relationships.

After discussing the three commonalities, I now address a unique content control operation for each country. My FoN analysis revealed that India's Cyber Crime

Volunteers Programme was used not only to monitor (as discussed in Subsection 6.1.1.1), but also to report illegal content to the police (see The Economic Times, 2021, as cited in India-FoN, 2021 in Section 7.1.1). This operation illustrates a panopticon mechanism, as it creates uncertainties over who is monitoring or reporting the content. Drawing on its closeness to the digital authoritarian literature discussed in Subsection 9.1.1.1, my analysis of the Cyber Crime Volunteer Programme suggests potential concerns about the democratic nature of the Indian government's operations online.

In contrast, the UK has multiple mechanisms for content control, which at times also act as oversight mechanisms over one another. These are the Internet Watch Foundation (IWF), Counter Terrorism Internet Referral Unit (CTIRU), and ISPs. Although they each control different aspects of content - the IWF focuses on child sexual abuse, CTIRU on terror content, and ISPs on copyright and child sexual abuse - I noted cases when these operations got intertwined. For instance, IWF provided support to ISPs regarding child sexual abuse content and CTIRU expanded ISP filters to remove terror content (see Mark; Wintour, 2014, as cited in UK-FoN, 2019-21 in Section 7.1.2). This not only differentiates the UK from India but also confirms its de-centralised approach to content control as part of its digital governance.

The above comparisons demonstrate not only the diverse range of players involved in content control operations, but also their adaptations to technology in India and the UK. This provides important findings about the countries' political approach to their digital governance, which contributes to the answer given to my main questions in Part 9.4.

9.1.3 Shaped Discourse

This section compares my shaped discourse findings on India and the UK. Drawing on the summary presented on Table 9.5, I discuss them in three subsections.

Table 9.5: Summary of shaped discourse operations		
	India	United Kingdom

Socio-political operations	• Political armies • Private firms	• Political parties • International interference • British Army
Significance of SMPs for discourse	• Traditional media • Political participation • Holds important power that is in the government's interest	• Important media channel • Power to direct information and technical features
Platform-specific discourse operations	• Facebook (advertisements and inauthentic behaviours) • Twitter (bots and trends)	• Facebook (advertisements) • Twitter (user-generated content, bots, trends)

9.1.3.1 Socio-political Operations in India and the UK

My findings reveal that shaped discourse operations were conducted by various actors in India and the UK. I compare them through three commonalities below.

The first commonality is that both countries had operations rooted in political parties during the 2019 elections. My findings on India reveal political parties' influence on SMP discourse through political armies, which were socio-politically and religiously motivated, as seen in the example of the BJP's head of IT Division, Amit Malviya (see India-FoN, 2019; Poonam and Bansal, 2019, as cited in Bradshaw *et al.*, 2021; Vikram in Section 8.1.1). This approach echoes a digital authoritarian practice discussed in the literature, such as '50 centers' being paid to support the Chinese regime online (see Diamond, 2010; MacKinnon, 2011; Bulovsky, 2019 in Subsection 2.2.1). In contrast, UK political parties engaged with disinformation, like the Conservative Party's doctored videos (see Kirka, 2019, as cited in UK-FoN, 2021 in Section 8.1.2), but also had small group which produced party-related content, like Momentum (see Satariano and Tsang, 2019, as cited in Bradshaw *et al.*, 2021, p. 415 in Section 8.1.2). One difference between the two countries is that, unlike India's political armies, Momentum lacked social and religious underpinnings. In spite of this, both countries exemplify the manipulative and targeted use of technologies by political parties

and the democratically challenging use of ICT technologies, especially during elections.

The second commonality is private firms and their role in shaping discourse on SMPs. While the UK was influenced by Cambridge Analytica's data-driven campaigning during Brexit, with debates over its potential links to the Conservative Party (see Cadwalladr and Graham-Harrison, 2018; Mance *et al.*, 2018 in Section 2.1.2), my research also identified the firm's involvement in India, where it worked with the main opposition party, the INC (see Siddique, 2019; Bradshaw *et al.*, 2021 in Section 8.1.1). This demonstrates how private companies have become integrated into political campaigning internationally and highlights their collaborations with diverse parties regardless of the context (ruling or opposition). Additionally, India was found to have engagements with another firm, Silver Touch. This was linked to a user whose posts had been removed from Facebook for spreading propaganda, but who was still active on the NaMo App (see Gleicher, 2019, as cited in Bradshaw *et al.*, 2021 in Section 8.1.1). Although NaMo exemplifies a loophole in platform regulation when compared to SMPs, this illustrates Facebook's efficiency in regulating content and disinformation on its platform. These findings underscore the diversity of private companies and operations they offer for different political actors globally, while also reflecting the growing proximity between technology companies and political processes discussed in Chapter 1 (see Kreiss and McGregor, 2017 in Subsection 1.2.1).

The third commonality is that both countries' discourse was interfered with and interfered in other countries. In India, Pakistan interfered with discourse on Kashmir and domestic political issues, while India interfered with the UK's discourse through the OFBJP's political army during the 2019 elections (see Nikhil; Siddique, 2019, and Canton, 2019, as cited in Bradshaw *et al.*, 2021 in Sections 8.1.1 and 8.1.2). While interfered with by India, the UK carried out military operations, both internationally - focusing on China and groups like Al-Qaeda - and domestically, like the 77th Brigade's Twitter monitoring during COVID-19 (see Emily and Carlo *et al.*, 2023 in Section 8.1.2). Despite having different political targeting, my analysis of the OFBJP shows the intersection of

my case study countries regarding shaped discourse operations in practice. Taken together, this meddling underscores the borderless nature of digital governance and dual usability of shaped discourse in becoming a digital tool and threat for state interference.

Unlike my previous themes, shaped discourse operations were not government-led but involved actors like ruling parties, opposition parties and other countries. Exposing these operations was important for comprehending the multi-stakeholder nature of digital governance in regard to shaped discourse and illustrating this theme's role at politically sensitive times like the 2019 elections. Keeping in mind that elections are common to both democratic and authoritarian regimes (see Chapter 2), India and the UK's manipulated and targeted discourse operations during elections demonstrates hybrid features of their digital governance (see Part 9.4 for more on this).

9.1.3.2 Significance of SMPs on Discourse in India and the UK

My respondents from both countries raised two key points about SMPs' significance for discourse.

First, they agreed that SMPs have surpassed traditional media outlets (see Vikram in Subsection 8.2.1.1, and Claire and Lauren in Subsection 8.2.2.1). Some argued that this shift had increased information availability and accessibility, as well as user participation on SMPs (see Priya and Nikhil in Subsection 8.2.1.1). Although these views align with the literature on digital democracy (see Dahl, 1989; Clift, 1998; Hague and Loader, 1999; van Dijk and Hacker, 2000; Berg and Hoffman, 2021 in Subsection 2.1.2), it contrasts with public opinion data from India, which show that 54% of people did not express a political opinion on SMPs (see CSDS-Lokniti 2019, p.18 in Subsection 8.2.1.2). This converse finding highlights the practical and contextual effect on how people engage with SMPs.

Unlike traditional media where sources and evidence are provided alongside information, my respondents from both countries shared a concern about the accuracy and reliability of information shared on SMPs. One UK respondent considered people's increasing reliance on information from SMPs to be worrying

(see Lauren in Subsection 8.2.2.1), while two Indian respondents questioned the accuracy of information on SMPs (see Nikhil and Tarun in Subsection 8.2.1.1). My data from the Indian respondents was further validated by CSDS-Lokniti's (2019, p.49 in Subsection 8.2.1.1) finding that only 25% of people trust the news seen on SMPs. Together, my respondents' observations on the shifting role of SMPs and the challenges this brings underscore the dynamic societal adaptation to changes from their contexts.

The second point was SMPs' power to shape discourse on their platforms. Respondents from both countries made references to advertisements, content curation and recommender systems, use of data to create patterns and trends, targeting, filters, and algorithms (see Sanjay, Nikhil, and Karan in Subsection 8.2.1.1, and Richard, Claire, and Jessica in Subsection 8.2.2.1). Some respondents viewed content which gets more clicks so brings in more money to the platforms as problematic, arguing that those items are usually misinformation, disinformation, propaganda, or fake news (see Nikhil in Subsection 8.2.1.1, and Richard and Jessica in Subsection 8.2.2.1). These opinions reflect not only the literature by Woolley and Howard (2018) about SMP-caused computational propaganda but also Fuchs (2024) and Andrejevic's (2011) observations on SMPs' capital driven structures that commodify user engagement (see Subsection 1.2.2). Taken together, these insights underscore the inorganic construction of discourse in the SMP ecosystem through the SMPs' features and financial motives.

My respondents' appraisals of SMPs provided valuable insights for grasping the role of SMPs and their relation to discourse in India and the UK. They discussed the platforms' technological features, illustrating a reflexive monitoring from the SMPs' standpoints and their duality relationship with the technology. Their comparison of SMPs with traditional media outlets emphasised the transformative and dynamic nature of SMPs, where they have become channels of spreading and obtaining information.

9.1.3.3 Platform-specific Operations in India and the UK

This subsection examines the technical features of Facebook and Twitter that my respondents assessed as influencing how discourse is shaped on SMPs. To discuss these in detail, I compare these two platforms' technical features in India and the UK separately.

Starting with Facebook, the most common feature my respondents raised was its advertisements (see Ravi and Amit in Subsection 8.2.1.2, and Tom and Lauren in Subsection 8.2.2.2). While the two Indian respondents expressed concern about Facebook offering cheaper advertisement rates to the BJP than other political actors (see Ravi and Amit in Subsection 8.2.1.2), the two UK respondents noted the uncertainty and complexity of advertisements created during the Cambridge Analytica scandal (see Tom and Lauren in Subsection 8.2.2.2). These viewpoints showed a similarity with other respondents who commented on the government-Facebook relationship. For instance, some Indian respondents had reservations about Facebook's close links with the BJP, such as Facebook's former Public Policy Head having prevented action being taken against a BJP member (see Ravi, Nikhil, and Vikram in Subsection 8.2.1.2). Meanwhile, my UK respondents highlighted Mark Zuckerberg's refusal to attend parliamentary questioning in relation to Cambridge Analytica (see Mark and Jessica in Subsection 8.2.2.2). However, one difference that appeared between the two countries is the change in government actions. While the BJP had shown continuous collaboration with Facebook despite widespread criticisms, the UK had taken formal steps to tackle problems arising from Cambridge Analytica's interactions with Facebook. That is not to say that problems with political campaigning on SMPs has vanished in the UK but demonstrates the government's reflexive efforts to address the issue within its digital governance.

Distinctively, my Indian respondents raised the issue of inauthentic activities on Facebook. One respondent noted that political armies' actions were by real users (see Vikram in Subsection 8.2.1.2), meaning that involving real users complicates the process of understanding inauthentic activities. Moreover, Facebook's selective removal of inauthentic activities shown many groups of users, including the INC, but did not report users from the BJP (see Gleicher,

2019; Gleicher, 2019, as cited in India-FoN, 2019 in Subsection 8.2.1.2). This not only builds upon views regarding Facebook's exclusive treatment of the BJP but also points out its potentially politicised controlling or reporting of inauthentic operations on the platform.

In regard to Twitter, one of the outstanding features my respondents raised was bots. Some respondents acknowledged various types of bots, with both beneficial and harmful uses (see Tarun in Subsection 8.2.1.2, and Jessica in Subsection 8.2.2.2). Others noted that bots do not participate in direct communications themselves but amplify the broader narrative through collective and coordinated operations (see Tarun in Subsection 8.2.1.2, and Lauren in Subsection 8.2.2.2). A further feature highlighted by a UK respondent was the role of users' organic and targeted engagement in political discussions on Twitter, particularly following the platform's removal of political advertising (see Emily in Subsection 8.2.2.2). This view confirms broader shifts caused by SMPs, showing how users who accumulate followers build an audience and become influential actors in shaping shape discourse. Another feature my respondents highlighted was 'trends'. While one Indian respondent remarked trends to be consisted of the exact same posts shared by many people (see Karan in Subsection 8.2.1.2), a UK respondent criticised them for shaping narratives on the platforms and influencing what is important for users to think (see Lauren in Subsection 8.2.2.2). Taken together, these points highlight my respondents' thoughts about three distinctive ways in which Twitter can shape users' discourse on the platform.

Unlike Facebook, Twitter was found to have tense ties with the Indian government. Both the FoN reports and one of my respondents (see Vikram in 8.2.1.2) highlighted incidents where Twitter's non-compliance with BJP-related matters had resulted in a backlash, including a court case and police visits. In contrast, my UK respondent did not raise any concerns about their government's relationship with Twitter. This highlights an explicit difference between India and the UK's digital governance of the two SMPs. Taking Facebook and Twitter together, my research findings reveal that India's digital governance of SMPs is

dependent on its control and collaboration with the platforms, demonstrating its politicised digital governance of SMPs.

Overall, my respondents' views on platform-specific features of Facebook and Twitter highlighted discourse-shaping activities that can originate by default from them. While this demonstrates the interpretative adaptations of these platforms with their technical features outlined above, my respondents' emphasis on their socio-politicised use denotes their dual usability and empirically reflects on the literature of computational propaganda within the contexts of India and the UK (see Woolley and Howard, 2018 in Subsection 1.2.3). This result led me to question the platforms' ecologies, since they have features which disrupt the natural construction of their discourse by default.

9.1.4 Summary

SRQ.1 investigated existing digital dual-use operations involving SMPs and their originators in India and the UK. Building on the comparative thematic discussions provided so far, I synthesise my answer through two points that directly address SRQ.1, and one emergent observation that contributes to the second part of the main question.

The first point is that both countries employed various digital dual-use operations on SMPs. These included government-linked tools, the integration of external technologies into governance, and their collaborative operations. Collectively, these practices demonstrate both countries' adaptations to emerging technologies, as emphasised in the literature (see Hague and Loader, 1999; van Dijk and Hacker, 2000; Deibert and Crete-Nishihata, 2012; Howells and Henry, 2021 in Subsections 2.1.1 and 2.2.1). Identifying these operations affirms that technology is not neutral - it holds a dual-use character and its affordances can vary in different contexts and actors (see Gibson, 2015; Hutchby, 2001; and Boyd, 2010 in Subsection 1.2.3).

My thematic findings show that -veillance and content control operations were linked either to central governments or in collaboration with external actors, whereas shaped discourse operations were mostly driven by political and

commercial motivations. This underscores the multi-stakeholder environment in which digital dual-use operations exist in India and the UK. The role of SMPs reinforces my thematic observation. Although Facebook and Twitter followed similar process in governments' user data requests, they differed structurally in terms of content removals and their stance on allowing political advertisements in their platform (see Section 5.7 for 'Limitations'). These structural differences influenced the platforms' roles in agency, like Twitter's capacity to act otherwise than what legal requirements and explains why it lacked political advertisement reports. From a digital structuration lens, this observation exposes technological dynamics among actors, their interpreted use of technology, and the conditions these interactions create for agency to operate.

The second point is that each of the thematic operations explored in this study - surveillance, content control, and shaped discourse - encompassed both technical and non-technical components. Technical operations consisted of institutionalised frameworks and state programmes, built-in features of the platforms, and tools developed or sold by private companies. Non-technical operations comprised the actions of certain groups, their strategic use of platform features, and informal relations among actors. This two-level consideration not only highlights the role of the government but also draws attention to other influential actors and stresses the interdependent relationship shaping digital-dual use operations. These dynamics also illustrate how platform affordances mediate the actions available to different actors (see Hutchby, 2001 and Boyd, 2010 in Subsection 1.2.3). My respondents' reflections on SMP-government relations further illustrated these dynamics. Some viewed their relationships as placing governments in a weaker position, while others emphasised SMPs' need to maintain cooperative relations in order to operate businesses effectively in the country. Taken together, this point demonstrates complex dynamics among governments, actors, and technologies, and their construction of the digital systems in India and the UK.

One observation that emerged from my digital dual-use operations findings is that how India and the UK integrated these operations provide insights about their digital governance regime. Although both countries have democratic state

governance, some of the thematic operations they conducted had a distinctly digital authoritarian character. For instance, India's purchase of spyware or filtering tools, lateral surveillance, pressure on SMPs, and the BJP's operations on SMPs, as well as the UK's policing and militarising of a civil environment, securitised use and development of tools, and politically motivated operations on SMPs are some of the non-democratic findings which carry digitally authoritarian characteristics. This does not mean that either country is digitally authoritarian but suggests a complex mixture of democratic system and undemocratic practice. This illustrates a problem of preserving democratic functionality (see Schmitter and Karl, 1991 in Section 2.1) when operating on SMPs, highlighting the deficit or hybrid features of thematic operations in India and the UK's digital governance (see Chapter 2 for democratic and authoritarian literature on hybrid regime). This observation provides an important bridge between my empirical findings on digital dual-use operations and shows that these operations carry significant implications for democratic practice and digital governance, which I examine further in Part 9.4.

In summary, my examination of digital dual-use operations identified various digital dual-use operations employed in India and the UK and highlighted the actors involved in them. Despite their contextual differences, I found that both countries have adopted and integrated technologies into their governments, engaged with other multi-stakeholders, and interacted with SMPs in ways that together shape their digital governance systems. Collectively, these dynamics reveal how structures, technologies, and agencies maintain mutually shaping relationships that unfolds digital governance in practice. In the context of digital dual-use operations, this triadic engagement foregrounds the relative causal primacy of technology, which is interpreted and engaged by structure and agency in the contexts of India and the UK. They also demonstrate the intricate interplay between democratic ideals and digital governance practices, which has laid the groundwork for answering the main research questions in Part 9.4.

9.2 Legal Frameworks and Concerns about the Regulation of Digital Dual-Use Operations and Stakeholders in India and the UK

9.2.1 -Veillance

Table 9.6 summarises my findings on the legal frameworks of -veillance in India and the UK. Following the order of the Table, I compare my findings in three subsections below.

Table 9.6: Summary of legal frameworks on -veillance		
	India	United Kingdom
Individual rights in relation to -veillance	• The Supreme Court decision over the right to privacy • The Right to Information Act (2005) • Digital Personal Data Protection Act (2023)	• Human Rights Act (1998) • Freedom of Information Act (2000) and the Freedom of Information (Scotland) Act 2002 • The Data Protection Act (2018)
State legislation governing -veillance	• The Indian Telegraph Act (1885) • The Information Technology Act (2000) and its allied rules	• Regulation of Investigatory Powers Act (2000) • The Investigatory Powers Act (2016)
Legal concerns about -veillance	• Consultation period • State-centric regulation	• Dual usability of law • Inadequate protection of rights

9.2.1.1 Individual Rights in Relation to -Veillance

Based on my review of the law regarding individuals' protection and their capacity to act, set out in Part 6.3, my research unearthed two commonalities between Indian and UK citizens' rights in regard to -veillance.

The first commonality is the right to privacy online. My introduction to Chapter 6 emphasised the importance of the right to privacy under Article 12 of the Universal Declaration of Human Rights (UDHR) (1948). Despite being written before the internet, its universal acceptance as well as its adoption by the two states illustrates the continued importance of the right to privacy. Although this

right is guaranteed under the Indian Constitution¹⁰² and the UK's Human Rights Act (1998)¹⁰³, it is not absolute in either country and can be limited within their respective definitions.

The second commonality is that both countries give their citizens the right to request information. This right enhances government transparency and citizen participation by allowing people to submit information requests to authorities on diverse matters, including their -veillance operations. It is guaranteed under the Right to Information Act (2005) in India and the Freedom of Information Act (2000) and the Freedom of Information (Scotland) Act (2002) in the UK. However, like the right to privacy, legislation in both countries contain limitations to these requests¹⁰⁴. Such limitations were reinforced by civil society actors, such as when SFLC's request on Pegasus was refused (see Subsection 6.1.1.2) and the incomplete response Privacy International received from local authorities in the UK (see Subsection 6.1.2.1).

Overall, while both countries have existing laws to preserve individual rights these are not absolute and can be restricted within the respective scope of the legislation. Thus, despite following a democratic process in making laws, I found that democratic principles were not being prioritised, for other reasons considered important for the state. It is important to highlight this point, since it raises questions about both countries' democratic functioning concerning their protection of 'civic rights', as pointed out by Schmitter and Karl (1991) in Section 2.1.

9.2.1.2 State Legislation Governing -Veillance

As outlined in Part 6.3 and depicted in Table 9.6, both India and the UK have laws permitting -veillance, including operations on SMPs. This subsection compares four commonalities in their legal frameworks.

¹⁰² See Subsections 6.3.1.1 and 6.3.2.1 for more detail.

¹⁰³ See Article 8 of the Act in Section 6.3.2.1.

¹⁰⁴ See Subsections 6.3.1.1 and 6.3.2.1 for more detail.

The first commonality is that both countries have laws on intercepting communications, which is important since this not only breaches the right to privacy but also require intermediaries to do so under the law. In India, interception is done primarily under the two pieces of legislation identified from my FoN report analysis - the Indian Telegraph Act (1885) and the Information Technology Act (2000). Similarly, two laws in relation to interception were identified in the UK - the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IP Act). While my findings on India show its centralised focus on intercepting domestic operations, the UK has different procedures for domestic and international operations, with domestic ones requiring stricter authorisation. This difference reveals the UK to have distinct -veillance governance strategy and stance when intercepting domestic and international communications. Additionally, unlike India, the UK has an Investigatory Powers Tribunal which acts as an oversight mechanism to operations conducted under the law.

The second commonality is data retention and sharing of those data with authorities. In India, the IT Rules (2021) governs this process, requiring intermediaries to store data for 180 days and outlines information sharing with the government (see Subsection 6.3.1.2 on the IT Act for more detail). Meanwhile, the UK's IP Act outlines a framework for 12 months of data retention and the need for a notice from the Secretary of State to obtain this information (see Subsection 6.3.2.2 on the IP Act for more detail). When compared, the UK requires data to be held twice more than India.

The third commonality is legislation on personal data protection. Although this was a shared finding, I observed significant differences in how this was framed in both countries. The UK's Data Protection Act (DPA) has been in place since 2018, while India did not pass its Digital Personal Data Protection Act (DPDP) until August 2023. Despite this five-year difference, India's DPDP Act is much more comprehensive and has been criticised for expanding government powers through its framework on data collection, processing, and creation of new government authorities (see Subsection 6.3.1.2). In contrast, the UK's DPA

focuses predominantly on the protection and legal processing of collected personal data, highlighting citizens' rights to rectification or erasure as well.

In sum, both India and the UK have several laws focusing on the controlling, regulation, and management of -veillance online. While India's legal frameworks illustrate a more centralised and government-empowering use of law, the UK takes a careful approach to domestic digital governance but simultaneously advances its comprehensive control in the international digital sphere. This comparative insight helps us comprehend the structural framework of their digital governance through the legislation and regulation of -veillance.

9.2.1.3 Legal Concerns about -Veillance

My respondents from both countries shared concerns about the law on -veillance. Because these concerns were thematically specific, I integrated public opinion data to interview data, which offered a broader contextual explanation that helped to situate their views within wider debates. The public data shows that 47% of Indians believe in fair treatment by the courts (see Devlin, 2019 in 6.3.1.3), while 62% expressed trust in the UK's courts and judicial system (see ONS, 2024 in 6.3.2.3). Acknowledging a relatively higher percentage in the UK, I now assess my respondents' one common and one unique concern regarding -veillance.

Respondents from both countries agreed that their countries lacked citizen-centric legislation when managing -veillance. My Indian respondents raised concerns about the inadequate protection of people due to the way the law was framed, and the lack of regulations that centred on people (see Amit and Vikram in Subsection 6.3.1.3). In the UK, my respondents primarily touched on the GDPR/DPA and shared concerns about its enforcement, inadequacy, and misuse of data (see Mark, Jessica, and Lauren in Subsection 6.3.2.3). Together, these concerns reveal my respondents' general dissatisfaction about their countries' frameworks on -veillance, and how these then influence people.

My respondents also expressed concerns that were unique to their country. For instance, two Indian respondents claimed that legal consultations were merely a

formality (see Sanjay and Vikram in Subsection 6.3.1.3), suggesting that India was ostensibly following a democratic process, but this was ineffective in practice. In contrast, a UK respondent assessed the two opposing uses of the law, like national security versus increasing surveillance (see Mark in Subsection 6.3.2.3), which provided interesting insights into dual-use workings of the law within a digital governance framework, as further explained in Part 9.2.4.

Taken together, my respondents' concerns expressed the resulting effect of the government's regulation of surveillance from agency perspectives. Keeping in mind that they can restrict individual rights in exchange for state regulation, my findings on India and the UK show that their digital governance holds both a democratic and non-democratic character, leading to a discussion about hybrid regimes in Part 9.4.

9.2.2 Content Control

Table 9.7 depicts the summary of my legal findings on content control in India and the UK. Following the order of the table, this section is divided into three subsections.

Table 9.7: Summary of legal frameworks on content control		
	India	United Kingdom
Individual rights in relation to content control	Freedom of speech and expression in the Indian Constitution	Freedom of expression in the Human Rights Act (1998)
State legislation governing content control	- The Copyright Act 1957 and John Doe Orders - Two allied rules of the Information Technology Act 2000	- The Copyright, Designs, and Patents Act (1988) and the Digital Economy Act 2017 - The Terrorism Act (2006) - The Online Safety Act (2023)
Legal concerns about content control	- Broad terms and politicised use of law - Over-regulation - De-prioritisation of individual rights	- Restrictions on individual rights - Specific issues with the Online Safety Bill

9.2.2.1 Individual Rights in Relation to Content Control

As noted in Chapter 7, Article 19 of the UDHR (1948) lists freedom of expression as serving an international normative foundation upon which I evaluate the two democracies' digital governance.

My findings set out in Part 7.3 show that both countries to have legislation on the right to freedom of expression and speech, but these rights are qualified. In India, freedom of speech and expression is guaranteed under Article 19.1.a of the Constitution but is limited in Article 19.2. Similarly, the UK grants freedom of expression in Article 10.1 of the Human Rights Act (1998) but limits it in Article 10.2. One difference between the two countries is the UK's ratified membership of the European Convention on Human Rights (ECHR) which requires its domestic legislation to comply with ECHR standards. Although this was criticised by a respondent due to the margin of appreciation doctrine of ECHR (see Claire in Subsection 7.3.2.3), it illustrates a unique difference as the ECHR provides an external mechanism controlling the UK's legislation, while India has no such mechanism.

In summary, both democracies acknowledge the right to freedom of speech and expression in their legal frameworks, but these are not absolute rights. This underscores the extent to which people in both countries might be protected and their capacity to act respectively. Such limitation also explains the importance of examining state laws separately.

9.2.2.2 State Legislation Governing Content Control

My research found two commonalities between India and the UK's state laws, and one unique finding specific to the UK on controlling content.

The first commonality is controlling copyright-protected content online. My reviews found that India has its Copyright Act (1957) and John Doe Orders to tackle this, whereas the UK has the Copyright, Designs, and Patents Act (1988) and the Digital Economy Act (2017). What differs between the two is that, while the laws in India focus primarily on protecting copyright materials and ordering

ISPs to remove content, the two UK laws entail a more comprehensive scope, covering not only copyright material but also child sexual abuse content. This difference confirms that the broad categorisation of the UK's legislation at times gets intertwined (see the below points as well), when compared to India's narrow way of tackling with issues.

The second commonality is controlling content through intermediaries. My FoN analysis identified two pieces of legislation in India - the Blocking Rules of 2009 and the IT Rules of 2021- and a newly-enacted law in the UK, the Online Safety Act (2023). India's laws provide a detailed framework covering request processes¹⁰⁵ and compliance periods¹⁰⁶, and require significant platforms¹⁰⁷ to have representatives living in India¹⁰⁸ and employ automated content removal¹⁰⁹ while operating in the country. Additionally, changes made in the IT Rules (2021) signal an increase in centralisation and the Indian government's power to control content. In contrast, while the Online Safety Act (2023) does not contain the contentious 'legal but harmful' provision from earlier drafts of the Bill (see Woodhouse, 2023, p. 77 in Subsection 7.3.2.2), it enforces intermediaries to use 'accredited technology' for content related to terrorist and child sexual abuse¹¹⁰. While both India and the UK's integration of technology into laws illustrate their adaptation from a structural lens, one difference between the two is that the UK also granted Ofcom as an oversight body under the Online Safety Act.

One particular finding that emerged regarding the UK is its controlling of terrorism content, under the Terrorism Act (2006). This Act not only focuses on direct and indirect terror encouragement involving SMPs but also covers content removal operations by the Counter Terrorism Internet Referral Unit (CTIRU)¹¹¹. Keeping in mind the UK's three broad categories in dealing with content -

¹⁰⁵ See Rule 7, Blocking Rules (2009) and Sub-clauses 3.1.d and 3.1.j of the IT Rules (2021); see Subsection 7.3.1.2.

¹⁰⁶ See the 48 hours' compliance period under Rule 8, Blocking Rules (2009) and 36 hours under Clause 3.1.d of the IT Rules (2021); see Subsection 7.3.1.2.

¹⁰⁷ Platforms with more than 5 million users (see India-FoN, 2021), in Subsection 7.3.1.2.

¹⁰⁸ See Sub-clauses a, b and c of Section 4 of the IT Rules (2021) in Subsection 7.3.1.2.

¹⁰⁹ See Sub-section 4.4 of the IT Rules (2021) in Subsection 7.3.1.2.

¹¹⁰ See Sub-clause 121.2.a.i of the Online Safety Act (2023) in Subsection 7.3.2.2.

¹¹¹ See Section 3 of the Terrorism Act (2006) in Subsection 7.3.2.2.

copyright, child sexual abuse, and terrorism - this legislation primarily covers the terror aspect of the country's legal frameworks on content control.

Overall, the above discussion shows Indian legislation to be more centralised and government-empowering when managing content, while the UK's approach is a more de-centralised form. These differences emphasise the role of the government and its potential interference in both countries when regulating social media content. Additionally, the fact that both countries passed legislation (such as the IT Rules in 2021 and Online Safety Act in 2023) on content control during my research period highlights the timeliness of this exploration and both countries' dynamic adaptations in their digital governance.

9.2.2.3 Legal Concerns about Content Control

Acknowledging the contextual background provided on public opinion in 9.2.1.3, this subsection compares two common legal concerns my respondents raised in regard to content control in India and the UK.

The first concern raised is the de-prioritisation and infringement of the freedom of speech (see Deepa, Amit, and Tarun in Subsection 7.3.1.3, and Claire and Mark in Subsection 7.3.2.3). Respondents from both countries shared a similar view on the extent to which speech should be regulated. My Indian respondents emphasised that free speech is regulable by pointing out the need to distinguish it from over-censorship (see Deepa and Priya in Subsection 7.3.1.3), while a UK respondent highlighted the legal basis on which such restrictions would take place (see Claire in Subsection 7.3.2.3). Despite their different interpretations, all three respondents' concerns reflect the extent to which freedom of speech should be regulated.

The second concern they raised relates to broad and vague definitions of the law when controlling content. My respondents from India cited some politicised interpretations of the laws and takedowns that are in the government's favour (see Ravi, Amit, and Tarun in Subsection 7.3.1.3). Additionally, one respondent provided the example of the Supreme Court striking out Section 66A of the IT

Act 2000 because it clashed with freedom of speech¹¹², yet there are still cases of this Article being implemented (see Tarun in Subsection 7.3.1.3). In comparison, the central issue UK respondents raised was the vague and broad definition of the Online Safety Bill's 'legal but harmful' provision (see David, Richard, and Claire in Subsection 7.3.2.3). Although the 'legal but harmful' provision was removed before the final Act was passed, their points illustrate the growing concerns in the making of the Act. While respondents' concerns illustrated the dual usability of broad and vague terms, the case in India displays a vital enforcement problem which has the potential to affect people's life and liberty, when compared to the UK.

Overall, considering the importance of freedom of speech for democracies, as highlighted by the UDHR and the literature (see Dahl, 2000, and Hague and Loader, 1999 in Section 2.1), my respondents' concerns illustrate its conditional nature in both countries. Their legal concern arising from the vague and broad definitions of law indicates the significant role of interpretation by the judiciary. Although both countries made certain changes that might have resolved these concerns, their outcomes differed -India faced the problem of implementing a Supreme Court decision, while the UK amended that provision during its Bill drafting. This difference illustrates the UK's closer following of democratic process and adapting a reflexive stance based on people's reactions, when compared to India's inadequate response to implementing the decision made by the highest judicial authority, Supreme Court.

9.2.3 Shaped Discourse

Focusing on my findings presented in Part 8.3, Table 9.8 provides a summary of the legal and government frameworks of shaped discourse in India and the UK. To compare and contrast them, this section is divided into three subsections.

Table 9.8: Summary of legal and government frameworks on shaped discourse		
	India	United Kingdom

¹¹² See FoN Reports (2021) for the case Shreya Singhal vs Union of India (2015); Subsection 7.3.1.3.

Individual rights in relation to shaped discourse	• Freedom of speech and expression • Freedom of religion in the Constitution • Election Commission	• Freedom of expression of the Human Rights Act (1998) • Freedom of thought, conscience and religion of Human Rights Act (1998) • The right to free elections in the Human Rights Act (1998)
State legislation and regulatory operations governing shaped discourse	• Indian Penal Code (1860) • Disaster Management Act (2005) • Internet shutdowns under the Indian Telegraph Act (1885) and the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules (2017). • Indian Election Commission	• Campaigns and RRU • Online Safety Act (2023) • ‘Disinformation and “fake news”: Final Report’ (2019) • Online Harms White Paper (2019) • Deepfakes and Audio-visual Disinformation (2019)
Legal concerns about shaped discourse	• Information regulation • Internet restriction as a way to regulate discourse	• Inadequate data protection to prevent discourse shaping • Individual rights

9.2.3.1 Individual Rights in Relation to Shaped Discourse

Unlike the previous themes, my research found only a vague consideration of protecting individual rights when it comes to shaped discourse. This was observed in both the rights listed under the UDHR (written before modern ICTs) and the two countries’ legislation. The most relevant UDHR principles for the targeting and manipulation of shaped discourse are freedom of thought (Article 18) and freedom of expression, which covers the right to hold opinions and receive information without interference (Article 19) (see Universal Declaration of Human Rights, 1948 in Subsection 8.3.1.1). To cover relevant aspects in both countries, I compare freedom of speech and expression, freedom of thought, and the right to free elections.

Although India and the UK permit their citizens to have freedom of expression, two key issues arise when they are compared within the shaped discourse perspective. First, both countries treat citizens' freedom of expression as a limited right, as was also explained in the content control theme. Second, there is a difference where the right considers 'interference'. Like the UDHR's Article 19, Article 10 of the UK's Human Rights Act (1998) considers 'interference' in terms of receiving information and sharing ideas, however, Article 19 of the Indian Constitution does not cover 'interference' at all. This reveals a contrast in how and to what extent these two countries have codified individual rights, as India does not protect its citizens against interference while the UK does protect them under its Human Rights Act.

Both countries guarantee freedom of conscience, religion, and thought for their citizens. The reason this was integrated into my discussions is because it reflects countries' democratic stance on citizens' ideas. This is guaranteed under Article 25 of the Indian Constitution, while the UK guarantees it in Article 9 of the Human Rights Act. Like freedom of speech and expression, these rights are also limited in their subsequent sub-clause; however, what is interesting about this limitation is that the UK's Subsection 9.2 states that this limitation is in the public interest, while India's Sub-clause 25.2 specifies religion, especially Hinduism. Considering that India is the most Hindu-populated country, this relates to the majority-minority division of the state and raises the issue of its secularity and equal treatment for other religions, especially when compared to the UK's approach to the public interest.

My research ascertained a difference in the right to have free elections in India and the UK. The UK codified free elections as an absolute right under Article 3 of The First Protocol, Part II, Human Rights Act (1998). This is missing from India's Part III on the fundamental rights provided for states and information regarding elections is only stated in Part XV, which is a detailed description of election proceedings by the Electoral Commission and the duties of the government. While this illustrates the UK's requirement to promote fair elections under the given absolute right, this is identified to be missing in India, meaning that free elections may not be guaranteed.

Overall, although no explicit rights cover shaped discourse directly, my analysis focused on freedom of speech and expression, freedom of conscience, religion, and thought, as well as the right to free elections in the two countries. The above comparison of individual rights reveals that both countries have old legislation in terms of being created before ICTs and SMPs. Hence, interpreting them within the dynamic nature of digital governance has illustrated some gaps and inadequacies in protecting individual rights online.

9.2.3.2 State Legislation and Regulatory Operations Governing Shaped Discourse

This subsection discusses India and the UK's legal and regulatory frameworks in controlling shaped discourse on SMPs. Unlike the previous two themes, both countries have some operational activities and, in contrast to India, the UK has some informal legal workings in regard to shaped discourse. To compare these, I focus on the one commonality and then highlight each countries' differences.

The only state arrangement commonality I identified in India and the UK is their management of discourse during public emergencies, like COVID-19. India has a specific legislation, the Disaster Management Act (2005), which was used by the Supreme Court to hold media outlets and intermediaries accountable regarding the information they shared on the pandemic (see Rajagopal, 2020, Chatuverdi, 2020, and Bindra, 2020, as cited in India-FoN, 2020 in Subsection 8.3.1.2). In contrast, the UK has run the SHARE and 'Don't Feed the Beast' campaigns and set up a Rapid Response Unit (RRU) to cope with misinformation online (see GOV.UK, 2020, as cited in UK-FoN, 2021 in Subsection 8.3.2.2). Although the UK's stance appears more progressive, both countries had some negative consequences. One Indian example of this was a health worker who was arrested for sharing an inaccurate number of COVID cases in Rajasthan (India Today, 2020, as cited in India-FoN, 2020 in Subsection 8.3.1.2), while in the UK, the military 77th Brigade monitored public perceptions of the Conservative Party posted on Twitter during the pandemic (see Carlo *et al.*, 2023 in Subsection 8.3.2.2). Thus, despite exemplifying how both countries regulated their online discourse during the pandemic, it also shows their influence on the public.

My thematic analysis of FoN data revealed that India and the UK have several differences. For instance, India has a criminal code, the Indian Penal Code (IPC) of 1860, and uses internet shutdown operations as part of its legal control involving SMPs. The IPC's criminalisation of discourse demonstrates some concerns regarding political misinterpretation, as seen in the arresting and detaining of journalists during farmers protests (see International Federation of Journalists, 2021 in Subsection 8.3.1.2). Additionally, internet shutdowns are conducted under two pieces of legislation, the Indian Telegraph Act (1885) and the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules (2017). Similar to India implementing the IPC during the CAA protests, a key incident integrated as an example from the FoN data evidence some local restrictions of the internet at the time of the CAA protests (see Subsection 8.3.1.2 for details of this example). Considering that this was a protest against the government for passing a discriminatory Act (see Subsection 3.4.1 for the context), these two ways of dealing with the discourse provide valuable insights into the government's intolerance of critical voices and its use of legal methods to silence them.

In contrast, my FoN analysis determined that the UK has the Online Safety Act and three government documents published in 2019. The Act's focus on managing illegal content represents one of the mechanisms through which online discourse is regulated in the UK. This legislation stemmed from the 'Online Harms White Paper', which set out the policy framework for creating legislation to ensure a safer online environment for people in the UK. The other two reports, 'Disinformation and "fake news": Final Report' and 'Deepfakes and Audio-visual Disinformation', demonstrate government efforts to address fake and tailored content. Despite these policy measures, the operations identified in my analysis also show political parties' disinformation operations and doctored videos during the 2019 general election (see Section 8.1.2 and Subsection 9.1.3.1 for the details and references). Although these two reports illustrate the government's policy efforts, they lack legal enforcements. Nonetheless, they indicate potential future regulatory developments, as exemplified by the Online Harms White Paper's progression to the Online Safety Act.

In summary, both countries have distinct documents (such as the IPC and DCMS reports) and operations (like internet shutdowns, campaigns, and the RRU). While these show efforts to adapt regulations to the digital sphere, they also raise democratic concerns. For instance, India's approach involves impacting on journalists' liberties and mass internet restrictions, while the UK includes surveillance of Twitter users. While these endeavours stem from different contexts and cannot be directly compared, they provide critical insights about the legal aspect and democratic context of SMP governance for each country.

9.2.3.3 Legal Concerns about Shaped Discourse

Building on public opinion of national courts discussed in 9.2.1.3, this subsection complements these broader patterns with my respondents' legal concerns regarding shaped discourse. They shared one common and several different legal concerns regarding shaped discourse in India and the UK.

Respondents from both countries emphasised information accuracy on SMPs. For instance, an Indian lawyer highlighted the importance of accurate information, while criticising the dominance of disinformation online (see Priya in Subsection 8.3.1.3). Meanwhile, a UK consultant distinguished between the right to information from the right to accurate information (see Sarah in Subsection 8.3.2.3). Her consideration of this distinction as an individual responsibility supports Ofcom's (2023, p.18 in Subsection 8.3.2.3) findings, which show that 41% of people verify information they see online. This means that, although the right to access information is seen as a democratic principle, it does not guarantee that the information will be accurate. This right is not only seen from legal enforcement positions, but also from platforms' content curation, which does not remove inaccurate content but does determine which content to amplify or silence (see Claire in Subsection 8.3.2.3). Considering that this feature does not fall under content removal or blocking since the content remains, it demonstrates the legal gap on regulating platforms through such subjective decisions over their content.

Aside from the above common concern, my respondents shared some different concerns in India and the UK. My Indian respondents observed a regulatory gap in

which these internet shutdowns were implemented, however, one respondent further highlighted the difficulty of regulating discourse and the government's potential discretionary use of it (see Tarun in Subsection 8.3.1.3). This viewpoint not only illustrated some personal distrust based on previous experiences but also aligns with 'the dual-use analogy' of how the legislation can be securitised in operations, as another respondent discussed (see Vikram in Subsection 8.3.1.3). Thus, respondents from India shared a concern on a regulatory gap, whilst also raising concerns about its regulation due to potential mis-regulations.

In contrast, a UK respondent emphasised the inadequacy of legal responses to using data for targeting reasons (see Tom in Subsection 8.3.2.3). Considering the Cambridge Analytica scandal experienced in the UK, the same respondent perceived the Data Protection Act to be inadequate. While this demonstrates an ongoing issue in the UK, it also shows a thematic interlinking of shaped discourse with -veillance (collection of data), which highlights the complexity of digital governance.

Overall, despite differing concerns, my respondents shared a dissatisfaction about their countries' management of shaped discourse on SMPs. This included the practical efficiency of the individual rights guaranteed under the right to access information, the difficulty of gaining accurate information, the technical regulation of platform features, and the creation of state legislation, reflecting on the shaping of legal aspects regarding shaped discourse.

9.2.4 Summary

SRQ.2 examined how legal frameworks in India and the UK informed the regulation of digital dual-use operations and stakeholders and explored the legal concerns surrounding their digital governance. This required not only evaluating the relevant individual rights for each theme, following my normative framework, but also considering other prevailing laws identified from the FoN reports, and my respondents' concerns. Based on the above comparative discussions, I summarise my answer to SRQ.2 by setting out two concepts that I developed from my study.

The first concept is the social construction of law when governing the digital sphere. By the social construction of law, I mean a state adapting its legal frameworks to digital governance. As Schauer (2005, p. 498) argued, the concept of law is socially constructed and continues to change over time, re-constructing itself. Considering the dynamic and mutually constituting aspects of digital governance system, of which structure is one (see Section 4.2), this concept reveals how legal frameworks in both countries inform the regulation of dual-use operation and stakeholders, as well as the protection and preservation of individual rights online. For instance, the summary tables provided on each of my thematic findings above show that both countries use laws that had been introduced before the publicising of the internet in the 1990s, like the Indian Telegraph Act (1885) or the Copyright, Designs, and Patents Act (1988). This not only indicates pre-existing frameworks but also highlights how they have been further interpreted to cover emerging technologies, the problems they created, and the multi-stakeholder networks generated. For instance, this is reflected in expansion of the Indian Telegraph Act's interception to include the internet and in how the Copyright, Designs, and Patents Act is applied to regulate the copyright materials online.

I also explain the social construction of law from how India and the UK introduced newer legislation that specifically governs the digital sphere. Both countries brought in new laws during my research period, including India's IT Rules (2021) and the UK's Online Safety Act (2023). These examples illustrate structural changes and adaptation to control digital dual-use operations (like data processing and content moderation), diverse intermediaries (like SMPs, ISPs, and MSPs), and individual rights (like the right to privacy in India and the data protection acts in both countries). Additionally, my interviews, which took place during the enforcement or ratification of Bills, provided insights about how the law is constructed. Some of my respondents explained how justified measures were implemented through practices like securitisation, how certain incidents had led to newer legislation, the strategic use of media, and the public normalisation of infringements caused by this legislation (like Arjun cited in Subsection 6.3.1.3, and Claire cited in Subsection 7.3.2.3). Thus, the social construction of law conceptualises dynamic changes from structural

perspectives. It informs how both countries' structures have shaped and constructed legal frameworks surrounding digital dual-use operations, stakeholders, and individual rights.

The second concept is the dual usability of law. Following my finding on how the law can be used both to protect but also restrict individual rights, I conceptualised this with dual-use characteristics. For instance, while the Indian Constitution and the UK's Human Rights Act promote their citizens' rights, both countries have other laws which restrict those individual rights online. This aligned with some of the legal concerns expressed by my Indian and UK respondents, like those who pointed out the dilemma of using the law either to protect citizens or to increase control over the digital sphere, the security implications these regulations create for citizens, and those who shared a broader concern about protecting rights online. Thus, this promotion and restriction of rights illustrate the two-way effect of law on the countries' digital governance, which I elaborate more below.

One aspect of the dual usability law is to guarantee individual rights. As I ascertained from my literature review, scholars from democratic fields perceived individual rights as a necessary part of democratic governance (see Schmitter and Karl, 1991; Dahl, 2000; van Dijk and Hacker, 2000 in Section 2.1), while those studying authoritarian regimes highlighted the undermining of individual rights as part of state governance (see Deibert, 2015; Yayboke and Brannen, 2020; Howells and Henry, 2021 in Section 2.2). My research ascertained that both India and the UK demonstrate efforts to protect relevant individual rights, like the right to privacy and freedom of speech, however, these are mostly qualified and can be limited. This reveals that both countries have a mixture of the democratic consideration of individual rights, but also practical ways to undermine those rights, just as in authoritarian regimes.

Another aspect of the dual usability of law is to restrict the protection and preservation of individual rights. For instance, both countries have laws that permit surveillance, encryption, content takedowns, data collection, and internet shutdowns, among other measures, which in turn limit their citizens'

right to privacy and freedom of speech. Some respondents argued that the primary legitimiser behind these restrictive laws was national security arguments. Considering the examples given on digital democracy (the US following Snowden's revelations, see Subsection 2.1.1), and digital authoritarianism (China's aim for international protection, Putin viewing the internet as a CIA projection, and Iran's goal to protect its moral values, see Subsection 2.2.1) reveals the securitisation over legitimising infringing operations in these two countries' context.

In summary, the social construction of law and the dual usability of law concepts inform us about the regulation of digital dual-use operations and stakeholders, and the protection of individual rights in India and the UK. Synthesised with my respondents' concerns, both concepts make an original contribution to the scholarship and complement my digital structuration framework. In this regulatory context, legal frameworks foreground the relative causal primacy of structure by explaining acceptable use of technologies and agentic practices, while simultaneously adapting to emerging technologies and evolving needs of stakeholders in both countries. Taken together, these findings also contribute to the main research questions of my thesis as these concepts address a complex situation where democratically processed laws have some non-democratic implications for individuals when regulating the digital sphere, raising the question of digital authoritarian effects. This confirms the point made in Subsection 2.1.2, where I cited Deibert (2015, p. 71) assertion that democracies which have restrictive laws on extremism and terrorism on the internet 'end up providing [the] biggest boost to resurgent authoritarianism'. While this mixture illustrates characteristics of a hybrid regime in the digital sphere, it also underscores the regulatory difference between governing in the real world and the online sphere, which will be articulated on more in Part 9.4.

9.3 Experts' Views and Concerns about the Implications of Digital Governance for the Indian and UK Public

9.3.1 -Veillance

Table 9.9 summarises my respondents' insights into awareness about and (dis)trust of -veillance, as discussed in Part 6.4. I discuss these by comparing two sets of findings on India and the UK below.

Table 9.9: Summary of views and concerns regarding -veillance		
	India	United Kingdom
Awareness	• Inadequate understanding and values adhered; material inequalities; lack of transparency	• Voluntarily given; increasing care after Snowden; public do not understand undermining democracy; normalisation
(Dis)Trust	• Democracy • The Indian government • Social media platforms	• Democracy • The UK government • Social media platforms

First, my respondents shared insights about the public's awareness of -veillance. Indian respondents cited unequal socio-economic opportunities and levels of education, a lack of common understanding of citizens' rights, and limited transparency as factors affecting people's awareness of -veillance (see Nikhil, Karan, and Arjun in Subsection 6.4.1.1). Their views aligned with the public opinion data from CSDS-Lokniti (2023, p. 219-158 in Subsection 6.4.1.1), showing that 84% had no awareness about the Supreme Court's judgement on the right to privacy and that only 25% of them had heard about the Pegasus spyware case. In comparison, two UK respondents emphasised increasing public awareness of -veillance, citing the Snowden revelations and the role of data during the COVID pandemic as the key reasons for this (see Jessica and Sarah in Subsection 6.4.2.1). While this aligned with public opinion data showing that 19% believed their data use would help during the COVID pandemic (see Centre for Data Ethics and Innovation, 2022, p.19 in Subsection 6.4.2.1), one UK respondent commented on the normalisation of -veillance at large and highlighted its impact on democracies (see Richard in Subsection 6.4.2.1). Except for one UK

respondent, who viewed the services provided to be in the public interest (see Sarah in Subsection 6.4.2.1), respondents from both countries were concerned about the public's inadequate understanding of the value and implications of -veillance.

Second, my respondents expressed three different levels of distrust regarding -veillance in India and the UK. These are distrust in democracy, in the government, and in SMPs, which I compare separately. Starting with democracy, public opinion data shows that 54% of Indians expressed democratic satisfaction (see Devlin, 2019 in Subsection 6.4.1.2), while only 33% were satisfied with democracy in the UK (see Electoral Commission, 2023 in Subsection 6.4.2.2). Although these percentages reflect different democratic environments, my respondents from both countries questioned and raised concerns about -veillance operations' influence on democratic rights (see Deepa, Ravi, Priya, Amit, Nikhil, and Karan on 'democracy' in Subsection 6.4.1.2, and Richard, Jessica, and Lauren on 'democracy' in Subsection 6.4.2.2). My Indian respondents expanded on this by focusing on how such distrust was leading to self-censorship (see Ravi and Amit on 'democracy' in Subsection 6.4.1.2), whereas the UK respondents explained their distrust through digital authoritarian discussions (see Richard, Jessica, and Lauren on 'democracy' in Subsection 6.4.2.2). Together, these reflections highlight a common view that -veillance is undermining democratic principles and has a non-democratic influence, leading to democratic distrust in India and the UK.

My respondents from both countries raised differing opinions about their distrust in government. To situate and validate this emergent finding within a broader context, I first draw on public opinion data. In India, 64% of people considered politicians to be corrupt whereas 55% were satisfied with the nation's direction (see Devlin, 2019 in Subsection 6.4.1.2). In the UK, 57% of people expressed little or no trust in the government (see ONS, 2024 in Subsection 6.4.2.2). These contextual indicators illuminate concerns raised by my respondents. My Indian respondents tied trust to one's political perception of the government, its use of national security as a justification for its undemocratic actions, and the misuse of dual-use operations, which they felt resulted in self-censorship (see Priya,

Sanjay, Vikram, and Arjun in Subsection 6.4.1.2). Their reflections aligned with the CSDS-Lokniti's (2023, p. 141-156 in Subsection 6.4.1.2) findings where 53% considered CCTV operations as justified for maintaining order and two-thirds feared a legal backlash for posting online. In contrast, UK respondents shared distrust in terms of the government's actions, its excessive operations under the national security argument, and its opposition to privacy and encryption, which had led some respondents to seek alternative solutions like self-censorship (see Tom, Richard, Emily, Mark, Jessica, and Lauren in Subsection 6.4.2.2). Their views aligned with public opinion data, showing that only 47% of UK adults trusted the government's legitimate use of data (see ONS, 2024 in Subsection 6.4.2.2). While respondents from both countries criticised their government's actions and operations justified by a national security rationale, India's case illustrated a more politically biased influence than the less politicised distrust regarding the UK government.

Lastly, my respondents raised distrust in SMPs, which I first contextualise through public opinion data. In India, CSDS-Lokniti (2023, p. 150-199 in Subsection 6.4.1.2) found that non-platform users expected higher surveillance intrusion than those who used platforms, and 70% believed their data was being accessed by other companies. In the UK, 8% viewed SMPs as a key issue in the country (see ONS, 2024 in Subsection 6.4.2.2). Although these figures relate to different aspects of SMPs and are incomparable, they help contextualise the setting in which my respondents shared their concerns. For instance, an Indian respondent commented on the reluctant use of certain SMPs due to their popularity, regardless of how untrustworthy the platform is in terms of surveillance or data management (see Nikhil in Subsection 6.4.1.2). In comparison, my UK respondents expressed distrust due to the power obtained by SMPs and its long-term consequences leading to self-censorship (see Mark, Jessica, and Emily in Subsection 6.4.2.2). This aligned with a general view of the public in the UK, where 56% of people consider political activities on SMPs to be inadequately regulated (see Election Commission, 2023 in Subsection 6.4.2.2). Taken together, my respondents' insights on the three levels - democracy, governments, and SMPs - alongside the public opinion data has exposed significant implications of surveillance on the public trust.

Overall, the findings show that public awareness and (dis)trust on -veillance are shaped by structure, use of technology, and platform-level dynamics, revealing digital structuration dynamics. While the public opinion data reflected a baseline among the two countries, my respondents' views on uncertainty, self-censorship, and concerns about democratic governance constructed aligning issues across two countries. Their reflections on self-censorship further demonstrated their reflexive thinking, illustrating agency's adjusting of their actions in response to the environment in which they operate. Together, these findings underscore the mutually reinforcing relationship between technology, structure, and agency in explaining how digital governance is constructed from the lenses of -veillance in India and the UK.

9.3.2 Content Control

Table 9.10 outlines a summary of my respondents' insights into the digital governance of SMPs from a content control perspective. I compare their opinions over three categories: general, specific groups, and self-censorship.

Table 9.10: Summary of views and concerns regarding content control		
	India	United Kingdom
General	Awareness Limited transparency due to law and secrecy in content operations	Normalisation of content control - Social construction of law - Infringement of democratic principles - Risk of digital authoritarianism
Specific people and groups	Impact on: - Political opposition - Journalists - Religious groups - Gendered experiences	Whose freedom of speech? - Freedom of speech may be abusive - One-sided interpretation and majority - Right wing
Self-censorship	- Potential backlash - Chilling effect - Organisational	- Not having control over data - Increasing awareness

First, my respondents' perceptions about public awareness of content control demonstrated a general level of assessment, which varied in each context. In India, my respondents described this through the limited transparency resulting from legal exemptions (like the Blocking Rules, 2009), which also influenced refusals of RTI requests by civil society organisations (like SFLC) (see Ravi, Vikram, and Karan, and India-FoN, 2020 in Subsection 7.4.1.1). This illustrates how legal frameworks influence public awareness of the Indian government's use of technology (like SFLC in the case of Pegasus). In contrast, my UK respondents highlighted the weakening of human rights by states since the two World Wars and 9/11, along with the perceived normalisation of infringements caused by content control and assessed it from a digital authoritarian lens (see Tom, Richard, and Claire in Subsection 7.4.2.1). While the historical point recalls the dynamics surrounding understanding of democracy across time, the latter reveals securitisation's effect on how governments control online content. Thus, unlike Indian respondents' views that regulatory mechanisms had the most impact on awareness, my UK respondents addressed how both regulations and content control operations were being normalised at a general scale.

Second, my respondents pointed out that certain people and groups had specifically been impacted by content control in both countries. Indian respondents described how users' political opposition, profession (journalists), religious beliefs, gender and sexuality created harms ranging from online trolling to arrests (see Deepa, Priya, Sanjay, Amit, Nikhil, Manish, and Karan, FoN reports, and other sources cited in Subsection 7.4.1.2). This demonstrates serious and threatening consequences of content control in the country. Although my UK respondents also described the role of gender, religion, and political views as specifically influencing those online (see Tom, David, Anna, and Lauren in Subsection 7.4.2.2), they questioned of whose freedom of speech content control protects, noting inequalities in its application. When compared to India, my UK respondents' concerns were seen to be less severe.

Third, my respondents raised self-censorship as a way to protect oneself online (see Sanjay, Tarun, Vikram, and Karan in Subsection 7.4.1.3, and Claire and Jessica in Subsection 7.4.2.3). In India, they thought this protection was needed

because of those who had been punished for posting certain content and to protect organisations for expressing opinions (see Sanjay and Karan in Subsection 7.4.1.3). Meanwhile, the UK respondents had reached this opinion highlighting reflexive consideration of users following scandals and not having control over content published online (see Claire and Jessica in Subsection 7.4.2.3). What emerged from my respondents' data in both countries is that self-censorship has become a reflexive pre-emptive and proactive tool for protection, which results in restricting the freedom of speech. These views complement Noelle-Neumann's (1974) spiral of silence theory discussed in Subsection 1.2.3 (see also Gearhart and Zhang, 2015 in Subsection 1.2.3), which explains how perceived social pressure can lead individuals to withhold their opinions.

In sum, my respondents' comments reflected multi-level assessments of content control in both countries. The broader level revealed a more comprehensive restriction and limited public awareness, while those raised on specific groups encompassed more targeted influence and self-censorship as a reflexive practice in society. Despite these similarities, it is crucial to clarify that the impacts discussed in India generated more serious harm at all three levels of society (especially at specific group levels) than in the UK. Taken together, my findings on content control provide significant insights about digital political regimes and the content control aspect of the digital system in relation to the context of agency in both countries.

9.3.3 Shaped Discourse

Drawing on the findings presented in Part 8.4, Table 9.11 depicts my respondents' concerns about the implications of shaped discourse on the Indian and UK public. I compare these matters in three categories below.

Table 9.11: Summary of views and concerns regarding shaped discourse		
	India	United Kingdom
General	Public discourse • Disruption of discourse • Impact on people's perceptions and opinions • Awareness	Limited awareness due to transparency of: • SMP operations • Political campaigning

Specific people and groups	• Activists and political opposition • Journalists • Women	• Women • Religious groups
Distrust	• Domestic democracy • International democracy	• SMPs • Domestic government • Democracy in theory and practice

The first impact my respondents highlighted was the influence of targeted and manipulated discourse on society. In India, 84% believed misinformation was being used as a weapon, while 75% reported the difficulty of identifying it (see Edelman, 2022 in Subsection 8.4.1.1). My Indian respondents echoed these concerns, describing how disrupted discourse affects individual and public opinions through polarisation and can be linked to serious offline consequences, including reports of innocent people being killed following the spread of doctored content and disinformation (see Sanjay, Amit, Nikhil, Vikram, and Karan, and FoN reports cited in Subsection 8.4.1.1). In comparison, UK respondents provided a narrower evaluation, commenting on SMPs' limited transparency due to their platforms' features and political parties' campaigning operations, which was tied to targeted advertisements influencing voters during the Brexit referendum (see Tom, Mark, and Lauren in Subsection 8.4.2.1). Their views aligned with wider public views, like 77% of people questioned the accuracy of information they see online (see Ofcom, 2023, p. 18 in Subsection 8.4.2.1), 68% had little or no trust in political parties (see ONS, 2024 in Subsection 8.4.2.1), 58% did not believe that party funding was transparent (see Election Commission, 2023 in Subsection 8.4.2.1), and 60% thought the regulation surrounding parties' campaign spending was inadequate (see Election Commission, 2023 in Subsection 8.4.2.1). Together, these assessments reveal digital governance's capacity to impact politics and highlight the difficulty and consequences of awareness in the two countries.

The second impact raised concerned how specific individuals were affected negatively. In India, respondents thought that the most affected people were activists and political opposition, journalists, and women. The impacts they mentioned ranged from the difficulty of spreading accurate information to

online harassment and receiving threatening phone calls (see Priya, Sanjay, Amit, Tarun, and Vikram in Subsection 8.4.1.2). In comparison, my UK respondents stated that women experienced trolling and some religious groups were considered extremists on SMPs (see Claire, Lauren, and David, and FoN reports cited in Subsection 8.4.2.2). Their views aligned with the wider public view in which 92% considered some users to act in ‘cruel or unkind’ ways on some platforms. This highlights a perceived difference between people’s behaviour online and offline. While my Indian respondents’ insights over shaped discourse aligned with the issues that existed at state level, the UK findings contrasted with its inclusive state context (see Chapter 3). Thus, counter to initial ideas that technologies would strengthen democracies (such as Clift, 1998 in Section 2.1), my empirical findings have shown that problems might remain (like in India) or get worsened online (as in the UK).

The third impact raised was (dis)trust in the management of discourse. My Indian respondents raised their distrust primarily through democracy. They referred to state level issues - like the ruling party’s operations conducted during elections - and issues at the international level, noting undemocratic practices in other democratic countries (see Ravi, Sanjay, Nikhil, Tarun, Vikram, Manish, and Karan in Subsection 8.4.1.3). Their insights resonated with public democratic satisfaction (54%), viewing politicians as corrupt (64%), and satisfaction with the country (55%) (see Devlin, 2019 in Subsection 6.4.1.2). In comparison, my UK respondents assessed distrust through platform management, the UK government, and democracy in general (see Emily, Mark, Anna, Jessica, and Lauren in Subsection 8.4.2.3). Their reflections aligned with the 20% who trust advertisements on Facebook (see Menlo Security, 2023 in Subsection 8.4.2.3) and 91% who manage advertisement options on the platforms they use (see Ofcom, 2023, p.24 in Subsection 8.4.2.3). They also complemented public opinion of 57% who had little or no trust in the government (see ONS, 2024 in Subsection 6.4.2.2), 34% who thought that technologies were responsibly regulated (see ONS, 2024 in Subsection 6.4.2.2), 56% think inadequate regulation of political activity on SMPs (see Electoral Commission in Subsection 6.4.2.2), and 33% who expressed democratic satisfaction (see Electoral Commission, 2023 in Subsection 8.4.2.3). Together, the analysis of my interview and public opinion

data show that distrust in discourse governance is beyond platforms or governments, pointing to a broader issue of the functioning of democracy itself in the digital sphere.

This shared democratic concern was evident across both counties. My respondents distinguished democracy in theory from democracy in practice, describing that what they had experienced in real life was different to the ideal perceptions of democracy itself (see Sanjay and Nikhil in Subsection 8.4.1.3, and Emily, Anna, Jessica, and Lauren in Subsection 8.4.2.3). Some perceived shaped discourse within democracies as a threat and harmful for the regime (see Sanjay, Nikhil, and Karan in Subsection 8.4.1.3, and Jessica and Lauren in Subsection 8.4.2.3). This not only reminds us of securitisation in the operations, but also their influence on democratic functionality, raising risks of hybridity in governance, as noted in the literature.

Overall, my respondents' observations on the public impact, alongside the public opinion data, highlighted the effects of operations, the role of SMPs, and the legal frameworks regarding shaped discourse. Their insights addressed not only the visible impacts on the public, such as severe harms due to disinformation or suppression of certain groups, but also the broader democratic concerns embedded in how digital spaces are governed in India and the UK. From a digital structuration perspective, these findings illustrate digital governance from the perspective of agency by reflecting on technology and structuration. Collectively, these findings offer significant contributions to my overall discussion on how India and the UK govern SMPs, as detailed in Part 9.4.

9.3.4 Summary

SRQ.3 explored the implications and concerns that digital governance creates for the public in India and the UK. Drawing on my comparative discussion of respondents' insights, alongside public opinion and secondary data, my answer to this SRQ can be summarised in three points: public awareness, impact on specific people, and distrust.

The first point is public awareness, which refers to how people understand existing dual-use operations, the broader SMP environment, and the legal framework surrounding digital governance. Public awareness emerged as a common pattern in both countries in relation to -veillance, appeared in content control analysis in India, and during shaped discourse discussions in the UK. This finding highlighted the need for equal development and collective understanding of democratic values by the public, alongside a more informed awareness of the challenges that dual-use operations creates for democracies. This public awareness finding also revealed uncertainty and a lack of transparency among actors involved, technology used, and how legal frameworks justified limitations. Although these constraints are not inherent aspects of the digital sphere, they are the observed outcomes of how digital governance has been constructed in India and the UK. This point demonstrates public awareness as part of digital structuration, reflecting on the ongoing interaction between operations (technology), institutional arrangements (structure), and the users navigating it (agency).

The second point concerns the impact encountered by specific people and groups, which were revealed in the content control and shaped discourse themes. My respondents from both countries described those affected, including political opposition, activists, individuals experiencing gendered backlash, certain professions (like journalists and politicians), and religious groups. While the severity of these impacts differed between the two countries, my analysis shows that these range widely, from online abuse to being arrested. These concerning outcomes indicate that rather than liberating citizens in authoritarian regimes, as Diamond had anticipated in 2010 (see Section 1.1), people experience restrictions and backlash people experienced within democratic regimes. This point reflects a broader challenge in contemporary politics, revealing how technology enables these dynamics and exposes the gap in the structural protection of democratic values within digital governance.

The third point is (dis)trust, which emerged from my findings on the -veillance and shaped discourse themes. The literature shows that trust between states and citizens was weakened by the Snowden revelations in the US (see van Dijck,

2014; Sørensen *et al.*, 2020 in Section 2.2). Although the literature refers to the US context, similar distrust dynamics appeared in India and the UK. My respondents expressed distrust in SMPs, governments, technologies, and democracies. Together, their insights related directly to the digital structuration framework and contextualised the digital governance system from democratic or authoritarian lenses. They also described self-censorship practices for users and certain organisations, indicating the reflexive monitoring of their agency and highlighting how users actively navigate and adapt to their governing conditions. This dynamic resonates with Noelle-Neumann's spiral of silence theory (see Gearhart and Zhang, 2015 in Subsection 1.2.3), in which perceived social pressure and declining trust might lead individuals to withhold their views.

In summary, the three points - public awareness, impact on specific people and groups, and distrust - capture my empirical findings on the observed implications and concerns of digital governance in India and the UK. Viewed through my digital structuration framework, these discussions highlight the relative causal primacy of agency by showing how technological operations and legal structures are interpreted, responded, and adopted by the public (including users, affected groups, and individuals) based on my respondents' perceptions and broader data analysis in both countries. In doing so, these findings also inform the main research questions of my thesis. Despite India and the UK both having democracy as their system of governance at the state level, my findings expose non-democratic implications that are important and insightful empirical insights about hybrid digital governance. Following my answer to the last SRQ, the next part of this thesis explains how India and the UK constructed their digital governance of SMPs and reflects on its implications for democracies and digital governance.

9.4 Digital Governance of Social Media Platforms in India and the UK: Structure and Political Regime

9.4.1 Digital Governance Structure: Empirical and Theoretical Perspectives

The answers provided to my three SRQs have revealed three constituent aspects that explain how India and the UK democracies construct their digital governance in relation to SMPs. These are:

- operations, defined as technical and non-technical practices of platforms, states, and other actors in the digital sphere;
- legal frameworks, understood as regulatory instruments that define the government's use and power over operations, regulate these operations and related intermediaries, and guarantee individual rights in the context of digital governance; and
- the observed implications on the public, which refer to the resulting impact of operations and legal frameworks on the public and the reflexive responses they generate.

These three aspects illustrate both the empirical outcomes of my inductive research and support my structuration model of digital governance framework. To provide a detailed discussion of each, I first focus on the three aspects of my empirical findings (see Figure 9.1) and then reflect on these with my theoretical framework (see Figure 9.2).

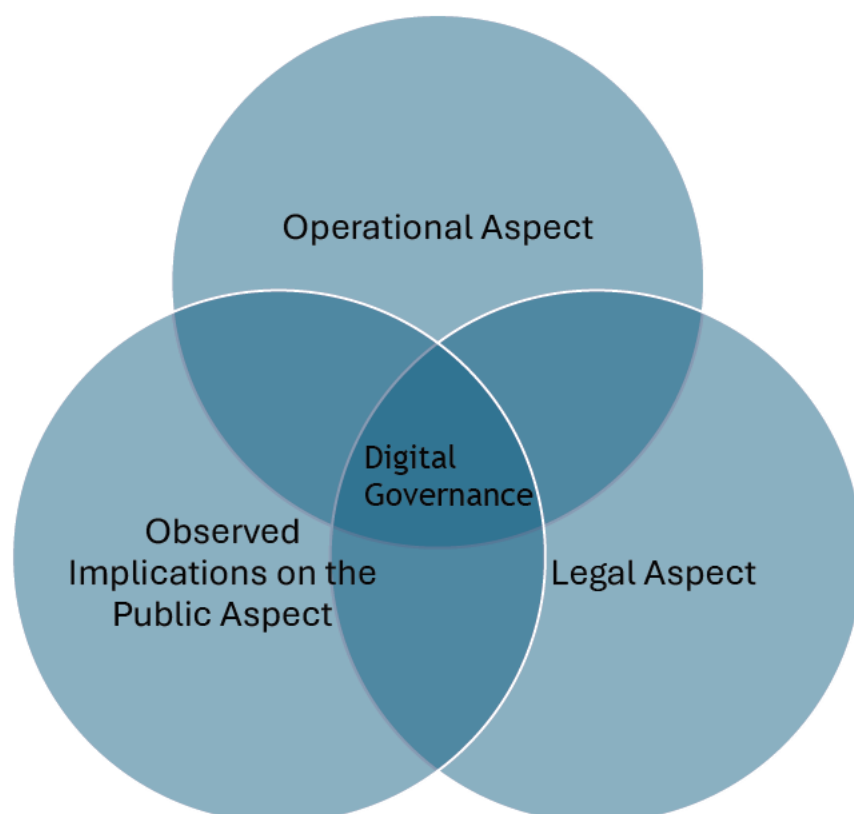
As discussed in Part 9.1, the operational aspect of digital governance covers the use of technical and non-technical operations that were ascertained in both countries. Identifying and understanding these operations revealed the roles and interactions among key multi-stakeholders, including governments, SMPs, and private firms. My findings show that this operational aspect can be a result of internal features of the platforms, as seen in Facebook's advertisements and Twitter's trends, but can also be interfered with externally, as shown in my findings on government-linked and collaborated operations. This suggests that the operational aspect comprises not only a mixture of technical and non-technical practices, but also a diverse source of operators, which collectively help construct the digital governance of SMPs in the two countries.

As discussed in Part 9.2, the legal aspect of digital governance is composed of regulating operations and stakeholders, as well as protecting individual rights online. My conceptualisation of the social construction and the dual usability of law is informed by both countries' regulation and to extent to which they protected individual rights. This illustrates how they construct the digital governance of SMPs from a legal lens.

Lastly, the concerns and implications identified in my research helped me to determine how the digital governance of both countries affects its people. Considering the complexities of operations and dynamics of the legal frameworks, this aspect comprises public awareness, implications on certain people or groups, and distrust in both countries. Despite occurring in both cases, my findings show that their extent and severity vary depending on countries' socio-political contexts and can be studied from different levels in societies.

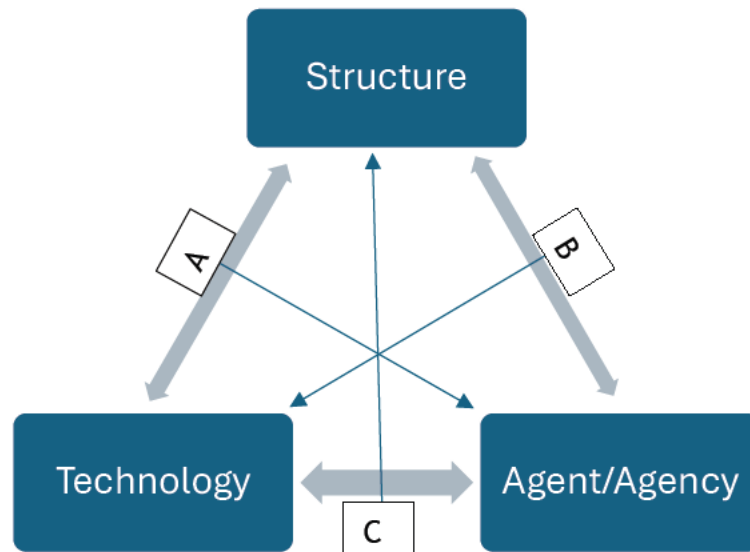
Taken together, these three aspects form the empirical constituents of how India and the UK have constructed their digital governance in relation to SMPs. Figure 9.1 visualises the three empirical aspects of digital governance discussed above.

Figure 9.1: The three empirical aspects of digital governance



Next, I integrated these three empirical aspects into my structuration model of digital governance framework. To achieve this, I refined the definitions of structure, agency, and technology given in Chapter 4 through my empirical findings. While doing so, I also reflected on their key features: their mutually constitutive (triadic) relationship, reflexive monitoring, and power. Figure 9.2 depicts this visually:

Figure 9.2: Structuration model of digital governance of social media platforms



First, structure depicts ‘domination and power’ through allocative and authoritative resources in SMP governance. Within the multi-stakeholder context of digital governance, structure consists primarily of state regulations and individual rights aspects, and the managerial aspects of SMPs, as my research has revealed. Governments maintain a duality relationship with agents and technology in the digital sphere. From the perspective of agency, governments protect individual rights and set legal frameworks to regulate SMPs. In return, they are influenced by the intentional actions of the agency, like the need to control people’s right to protest against the government or to create mechanisms to deal with SMPs’ non-compliance. From the technology standpoint, governments not only regulate technologies in the digital sphere, but they are also influenced by interpreted use and the integration of technologies into their systems, like legally requiring an automated filtering tool for content control in India and the UK.

When viewing SMPs as structures, their duality relates to the policies they create to regulate their platforms. From an agency standpoint, this includes both how they manage users on their platforms, and how the platforms evolve and constantly adapt to their users' behaviours. From a technological standpoint, this refers to SMPs purposing technical features on their platforms, like Facebook advertisements or Twitter bots, but also the consequences of these developed technologies in terms of influencing their socio-political environment, depending on the context and interpretative use of these technologies. These dynamics underscore the triadic relations of digital governance from a structural standpoint and highlight the importance of interpretation and context, as explained in the next paragraph.

Considering the dual usability of technologies discussed in previous chapters, structure has the power to interpret and use technology. Thus, depending on the structure's interpretation of technology (this can be either from the government or the SMP), it can influence the agent in various ways, like controlling what information people can see, or shaping public discourse (see arrow A between technology and structure, pointing to the agent in Figure 9.2). Similarly, the structure's duality engagement with agency can influence technology, since people can have reflexive monitoring (see arrow B). This was seen, for instance, in the UK when people quit Facebook after the Cambridge Analytica scandal, or some users started self-censoring on platforms following the arrests of journalists in India. Once again, this highlights the triadic relation of structure with technology and agency in the digital governance of SMPs.

Second, agency shapes the structure and the technology through its mutually constitutive relations, power, and reflexive monitoring. Agency, within the context of my research, mainly involved people with the power to act and make decisions intentionally (see Giddens, 1984, pp. 5-16 in Subsection 4.2.1), which includes broadly the public, people like my respondents and their references to groups (including users, minority groups, and the public in general), as well as SMPs. From a structural standpoint, agency can be understood by the ways people voted in elections to form a government or raised issues to influence government policies. This, in turn, influences state policies on digital

governance. From a technological standpoint, agency/agents use platforms and shape them through their behaviour, while the platforms and technologies influence them back, for instance, through shaped discourse activities or as a result of incidents and reflexive monitoring, leading to self-censorship.

When considering SMPs as agent/agency, my study has demonstrated that SMPs have the power to intentionally determine and respond to the structure (governments), as seen in my transparency report analysis which showed that Facebook and Twitter had both denied and complied with government requests. This, in return, creates a duality relation with the structure, where the government can respond in return. One example of this was the Indian government's relationship with Facebook and Twitter and the consequences Twitter faced when operating against the BJP's interest, like being subjected to a police search. From a technological standpoint, SMPs (as agencies) develop technologies and integrate them through their own interpretations, while such adaptation in return changes their design, as seen in Twitter's removal of political advertisements in 2019 and the observations my respondents made on the platform's changing algorithms following Elon Musk's arrival in 2022.

Considering the interplay between these three aspects, the agency's duality with technology and structure not only shapes those two but also influences them back as well. For instance, agency influences which political actors form the government through elections. This, in turn, decides the ideology of the government that would interpret and use technology in a country, like the internet shutdowns in India or developing collaborative projects in the UK (see arrow B). Similarly, the agency's duality with the technology influence structure was seen in points like creating legal requirements for controlling illegal speech (like the discussions over the OSB in the UK), or arresting critics of the government in India (see arrow C). Thus, this demonstrates the triadic interplay within digital governance of agent/agency with the structure and technology on SMPs.

Third, both the structure and the agent are consistently affected by the duality of technology. In my research I found that technology mainly consisted of the

technical and non-technical operations involving SMPs (see SRQ.1). From the structural standpoint, technology shapes the ways governments and SMPs operate in the digital sphere (like infrastructural programmes, technical, and non-technical operations and features). In return, this reflects how they design their regulations and policies to manage it, aligning with Orlikowski's (1992) point those technologies become 'institutionalized' (see Subsection 4.2.2). From the agent/agency standpoint, technology is developed and interpreted by humans (as Orlikowski argued) and can be influenced by different contexts (as asserted by Walsham, 1993), but the implemented operations also affect people in return, like through bots or advertisements. From the SMP standpoint, where SMPs are both the agency and the technology, platforms not only possess technological features (like Facebook's advertisements and Twitter's trends), but are also subject to other technologies, as my empirical findings have demonstrated how the two countries were influenced by external technologies as well.

This means that technology's influence on agency affects the way it gets regulated by the structure (see arrow C), as discussed regarding protests that began on SMPs and resulted in the government needing to control agency (like the CAA or farmers' protests in India), or externally-applied technologies on SMPs requiring a parliamentary investigation, like the Cambridge Analytica scandal in the UK. Similarly, technology's duality with structure influences the agency, like Facebook's cheaper advertisements for the BJP in India which were expected to influence its users, and the UK's automated filtering tools on service providers to pre-emptively filter the content published on SMPs (see arrow A).

Despite the different aspects integrated, my structuration model represents how these three interdependent elements have a triadic relationship that shapes and constructs the digital governance of SMPs. While these elements remain mutually constitutive, as also described in Subsection 4.2.4, my analysis demonstrates that the relative causal primacy of structure, agency, and technology can shift across empirical contexts, depending on which aspect of digital governance is discussed at a given moment. Taken together, this

framework provides a holistic understanding of the complexities of digital governance and considers the socio-political and historical contexts in which countries play a significant role in influencing the social systems of digital governance. This not only underscores the importance of context and interpretation, but also confirms my differing contextual findings identified from the interplay of technology, structure, and agency in India and the UK.

9.4.2 Digital Governance Regimes in India and the UK, and the Emergence of a Digital Hybrid Regime

Another way to explain how India and the UK constructed their digital governance of SMPs is through articulating their digital governance regime, which further helps elaborate on the significance of this for democracies and digital governance. My comparative discussions have highlighted digital democracy and digital authoritarianism signals in both countries. Connecting these mixed regime findings with the literature leads to a discussion about hybrid regimes. My research reported in this thesis discovered that both India and the UK have a *digital hybrid regime* on SMPs. To explain this, I focus on the democratic and authoritarian features I observed within the two countries.

First, scholars from democratic fields have perceived digital democracy as the expansion of state democracy and its practices into the digital sphere (see Hague and Loader, 1999; van Dijk and Hacker, 2000; Simon *et al.*, 2017 in Chapter 2). One way to discuss this from a digital hybrid regime perspective is by recognising that both countries have a democratic system of governance at the state level. Despite India and the UK's different political contexts (see Section 3.2), my research found democratic procedures in their governance pertaining to the digital, primarily through making laws and regulations encompassing SMPs and their public¹¹³.

Another democratic feature that emerged from my study was the expansion of democratic practices on SMPs by the two countries. My empirical findings addressed political participation and access to information on SMPs¹¹⁴, as

¹¹³ See Part 3 of -veillance, content control, and shaped discourse chapters or SRQ.2 (9.2).

¹¹⁴ See Part 8.2.

emphasised by some scholars in the digital democracy literature (such as Dahl, 1989; Clift, 1998; van Dijk and Hacker, 2000; Simon *et al.*, 2017; Berg and Hoffman, 2021 in Chapter 2). Furthermore, both countries have legislation intended to expand their citizens' access to information, like the Right to Information Act (2005) in India and the Freedom of Information Act (2000) in the UK. These two features demonstrate that both technological and state adaptation play a role in expanding democratic practices on SMPs in India and the UK.

Second, I summarise the digital authoritarian elements I identified in my research into the digital governance of SMPs in India and the UK. As detailed in Subsection 2.2, some of the tools referred to as digital authoritarianism in the literature include censorship, surveillance, manipulation, and content control (see Section 2.2 for more details). Additionally, the countries named as examples of digital authoritarianism in Chapter 2 illustrate the strategic use of law as part of their regimes (see MacKinnon, 2011 and Deibert, 2015 in Section 2.2). I revisit this literature here because my empirical findings have unearthed some innovative links with India and the UK's digital governance, as explained below.

As discussed under the realm of SRQ.1, my case countries used surveillance, dataveillance, external tools, content takedowns and blocks, manipulation, and user targeting on SMPs. Despite the literature's emphasis on and labelling of these tools as forms of digital authoritarianism, my case studies have exemplified their use in democracies. This not only cautions against categorising dual-use operations as exclusively authoritarian but also shows their adaptation in the two democratic countries.

Another point that showed some alignment between my findings on India and the UK with the digital authoritarian literature is in relation to the use and construction of law. As discussed, regarding SRQ.2 and SRQ.3 above, the law plays a crucial part in digital governance in terms of regulating and protecting individual rights, exposing some non-democratic implications including the infringement of individual rights and influencing free and fair elections.

Considering the examples of China, Russia, and Iran's use of law illustrates these digital authoritarian concerns. Moreover, some respondents raised concerns about states using 'national security' and other securitising elements as rationales to legitimise imposing extraordinary measures.

Overall, my discussion on political regimes and India and the UK's digital governance of SMPs reveals neither a full digital democracy nor a complete digital authoritarianism, but instead a mixture of the two, a digital hybrid regime. Considering the different definitions and approaches democratic and authoritarian scholars have taken on hybrid regimes in the literature (see Chapter 2), I follow Gilbert and Mohseni (2011) in constructing a definition of digital hybrid regimes in Chapter 10.

9.5 Conclusion

Drawing on my research findings presented in Chapters 6 to 8, this chapter has provided a comparative discussion of India and the UK through the lens of my research questions. The initial three parts centred on my SRQs, providing a comprehensive and multi-dimensional discussion of the digital governance of SMPs in India and the UK. In doing so, it exposed the interplay between governments, SMPs, law, private firms, technology, and people, reflecting on my digital structuration framework. While these discussions have highlighted the intertwined construction and shaping of the digital sphere, they have also revealed some connections to the state contexts detailed in Chapter 3. This not only demonstrates state influence on the digital sphere but also shows some alignment with the issues experienced by users and the general public, like the specific impact observed on certain groups. Drawing on the answers given to three SRQs, Part 9.4 answered main research questions of my thesis. This involved outlining empirical and theoretical designs in reflection to my digital structuration framework and discussing on the complex political regime observed in both countries. Following this, the next chapter develops the digital hybrid regime concept in more detail and concludes this thesis by outlining my research reflections.

Chapter 10 Conclusion

The primary aim of my research was to understand how Indian and UK democracies have constructed their digital governance in relation to social media platforms, and to further assess the broader significance of this for democracies and digital governance. My study has achieved its objectives outlined in Chapter 1 by examining digital dual-use operations, legal frameworks, and respondents' key concerns about the digital governance implications on the public in India and the UK. Building on my findings presented in Chapters 6 to 8 and the discussions in Chapter 9, I have proposed a novel digital governance structure and developed a new concept of 'digital hybrid governance', one of the primary contributions of my thesis, which will be expanded on in this chapter. Thus, this chapter is divided into two parts. Part 10.1 provides a definition, develops a conceptual framework, and introduces a typology of digital hybrid regimes. Part 10.2 reflects on the research outcomes, including research contributions, policy recommendations, limitations, and recommendations for further studies. I conclude my thesis with some final remarks.

10.1 Digital Hybrid Regimes

I define a digital hybrid regime (DHR) as a **unique form of digital governance that has a mixture of digital democratic and digital authoritarian elements**. To develop this definition further, this part is divided into two sections: 'Digital Hybrid Regime' as a new concept in digital governance, and the three types of digital hybrid regimes.

10.1.1 'Digital Hybrid Regime' as a New Concept in Digital Governance

The literature review provided in Chapter 2 showed that a hybrid regime lies in the midpoint between a democratic and an authoritarian regime. To discuss its evolution in digital governance, I start by clarifying the hybrid definition of state governance and then explaining how I constructed my definition, building on the digital governance literature reviewed.

As discussed in Chapter 9, I follow Gilbert and Mohseni's (2011) approach to hybrid regimes. Instead of viewing India and the UK's digital governance of SMPs as being illiberal or semi-authoritarian, this approach conceptualises a digital hybrid regime as a separate form of digital governance, in addition to the existing dominant literature on digital democracy and digital authoritarianism.

Although most discussions of hybrid regimes focus on state-level governance, Wright (2019, p. 31) categorises China as a digital authoritarian state, the US as a digital liberal democracy, and Russia as a 'digital hybrid regime'. She classifies Russia as a hybrid regime since it has both democratic state governance and some digital authoritarian elements (see Section 2.2.1). However, considering digital democratic concerns raised about the US in both the literature and my research findings, as well as Russia's authoritarian tendency at a state level, I took a different approach to defining a digital hybrid regime than Wright (2019). Instead of mixing state governance with digital governance to construct a form of digital hybrid governance, I viewed digital governance as a separate level of governance that is only partially affected by state governance, especially due to regulatory mechanisms. That is, I did not mix democratic state with digital authoritarian actions to construct a digital hybrid regime. I justified this approach using the structuration model of digital governance set out in Chapter 4 and expanded on in Chapter 9, and by highlighting the interplay on digital governance. Thus, I distinguished digital governance from state governance and argued that it is a separate form of governance which can differ from the regime a country practices at state level. Before introducing a typology showing how different state regimes can have digital hybrid regimes, I first outline the three constituting aspects used to build a conceptual framework on digital hybrid regimes.

To construct this conceptual framework on digital hybrid regimes, I integrated the empirical model developed in Section 9.4.1 and built on it through three constituent elements: operational, legal, and observed implications on the public.

The first component of a digital hybrid regime is the operational aspect. As detailed in Parts 9.1 and 9.4, this includes technical tools and non-technical operations on SMPs, which helps to explain a digital hybrid regime in two ways.

First, technical tools refer broadly to the dual-use operations conducted on SMPs. Focusing on the thematic operations of -veillance, content control, and shaped discourse, my research has confirmed the importance of dual-use technologies on SMPs (as noted in Chapter 1) and pointed out their democratic and non-democratic implications, using my two case studies. Therefore, dual-use operations constitute one of the significant factors of hybridity, indicating technologies' mid stance in having conflicting implications. Another constituent element of technical tools is the power imbalance created by multi-stakeholder actors in digital governance. This not only highlights the state's loss of power monopoly over operations but also emphasises the diverse range of actors who hold operational power online. This reveals not just the power and role of SMPs in technical operations like advertisements and bots but also shows that private companies and externally developed tools are part of digital governance. The reason my research considers this to be a hybrid element is that, because government purchases from private firms cannot be tracked, this limits transparency and creates secrecy and uncertainty about operations conducted by states. In addition, I have identified this imbalance as a factor in determining a state's objective of regulating these firms, due to their dependency on them. Put differently, a state's dependency on other stakeholders and the problem of transparency about their collaboration illustrates some characteristics of the digital hybrid model my research has produced.

Second, non-technical methods include operations that are conducted online manually by humans without employing technical tools. One of the most prevailing examples I have detailed is the kind of operations that are conducted in coordination with a group of people, like political armies in India and Momentum in the UK. Despite their difference in size, both of these demonstrate a coordinated operation online and consist of real people working for political purposes. Going further than simply talking about coordinating people online, states can also create special programmes within their system

and employ other types of non-technical operations, as was seen in the lateral surveillance by India. The reason for coding these non-technical operations as a hybrid form was because my empirical findings showed their use in targeting SMPs on socio-political issues, affecting not only deliberative and accurate discourse but also risking individual rights. Moreover, both these examples demonstrate states creating uncertainty about what information to rely on and who to trust for monitoring reasons on SMPs.

The second component of a digital hybrid regime is the legal aspect. As detailed in Parts 9.2 and 9.4, this required understanding not only a country's individual rights and laws, but also its roles in digital governance. To explain and construct the digital hybrid regime concept in terms of legal aspects, I drew on the social construction of law and its dual usability.

First, I have explained the social construction of law in digital hybrid regimes through the securitisation of strict laws and states' law-making processes. Securitisation, as defined in Chapter 1, not only shapes the audience's perception of a new threat but, in doing so, justifies the extraordinary measures taken by political actors. Building on this, I expand my argument on the social construction of laws in digital hybrid regimes to argue that a digital hybrid regime may not have either dictatorial laws like authoritarian regimes or an idealistic approach like democracies, but it can socially construct restrictive laws that are accepted by the public, who consequently give up their rights and accept restrictions. Based on my research findings on India and the UK, I posit that this can take place regardless of whether a democratic law-making process is followed. By a law-making process, I refer to a state's legislature process and the separation of government powers¹¹⁵ that is evident in democracies. In other words, following a democratic process does not prevent rulers from making strict laws within states. One of the most prevailing examples in this regard was the 'national security' arguments I have detailed in my findings on India and the UK. Thus, the social construction of law is a vital aspect of a digital hybrid regime, as it clashes with the primary features of democracies, including individual

¹¹⁵ Legislature, judiciary, and executive branches of government; see Chapter 3 for context on these countries.

rights and freedoms, but at the same time it is not authoritarian because it follows a democratic procedure. That is why my research considers the social construction of law to be a component part of digital hybrid regimes.

Second, the dual usability element of digital hybrid regimes refers to the laws that are in place to protect people, but which can, nonetheless, cause harms to them. I built this duality concept based on the dual-use technologies discussed in Chapter 1. I argue that, like dual-use technologies, the law can be used for both good and bad for people in digital hybrid regimes. By the good, I mean to protecting citizens within the scope of the law, while the bad refers to both the harmful impacts the law can have on people as well as its potentially politicised use by people in power. For instance, India and the UK's online freedom of speech is limited by the Intermediary Guidelines of the IT Act (India) and the Online Safety Act (the UK). Another example of the politicised use of law was given on India's terror law (the Unlawful [Activities] Prevention Amendment Act), which was used to arrest several journalists who posted on social media against the ruling government in India¹¹⁶. Therefore, the duality character of the law creates a grey area where it can be used either way by those in power, leading to a digital hybrid regime.

The third component of digital hybrid regime is the impact of the operational and legal aspects of digital governance on the public, as asserted through the concerns and implications observed by the respondents I interviewed in my research. Considering the dual usability of technologies and the law, this aspect illustrates the resulting effects it generates on the public, whether these are democratic or authoritarian. To explain this within the context of digital hybrid regimes, I focus on two elements derived from my empirical findings on the observed implications on the public: public awareness and public trust.

Public awareness is people's general knowledge about operations and understanding of legal frameworks in relation to digital governance in their country. This covers not only basic digital literacy, but also transparency and the government's educational efforts to help improve people's understanding. While

¹¹⁶ See Subsection 7.4.1.2.

the ideal perception of a democracy is associated with transparent governance (Gorwa and Ash, 2020), in contrast to an authoritarian regime which demonstrates some censorship (Deibert, 2015; Howells and Henry, 2021), my empirical findings show that public awareness occupies a nuanced ‘grey’ position within a digital hybrid regime. I have shown how, in a developing country like India, the unequal educational and economic opportunities within society affect public awareness of digital governance¹¹⁷. Meanwhile, in a more developed country like the UK, public awareness of the values adhered to in digital governance was evident in the normalisation of non-democratic implications and the public acceptance of government-proposed solutions to problems arising¹¹⁸ in the digital sphere. What was common between the two was the formal image of a government that was idealistic, which contrasted with what I observed in practice during my study. Moreover, digital hybrid regimes, such as these two countries, contain groups of people who are calling for more transparency and working to increase public awareness. Overall, public awareness develops to some extent in digital hybrid regimes, but not as far as it would in a digital democracy.

Public trust is an important feature of the relationship between a government and its citizens, whether in a democratic or authoritarian system (Warren, 2018). However, my study identified distrust as one of the key factors constituting digital hybrid regimes. Taking into account the multi-stakeholder characteristics of digital governance, my research assessed trust at different levels - the government, SMPs, technologies, and democracy as a system of governance. This comprehensive consideration is important for understanding not only a country’s public trust in its government, but also its management and control of other multi-stakeholders in the digital sphere. The data I gathered from respondents who were experts in India and the UK found that their experience of SMPs had fostered a general distrust in most of the themes, illustrating the role of distrust in digital hybrid regimes.

¹¹⁷ See Nikhil in Subsection 6.4.1.1.

¹¹⁸ See Richard and Sarah in Subsection 6.4.2.1.

In sum, the concept of a digital hybrid regime is composed of three aspects: operational, legal frameworks, and observed implications on the public. Resulting from my empirical findings, these aspects provide a common characterisation of the digital hybrid regime concept. This concept was built on the basis that digital governance differs from state governance, despite being affected partially by it, through factors like its laws. Having produced this distinction between state and digital governance allows me to introduce a typology of digital hybrid regimes, where state regimes adopt different digital hybrid regimes.

10.1.2 Three Types of Digital Hybrid Regimes (DHRs)

This section outlines three types of digital hybrid regimes which differ in the type of state governance that adopts them. To create this typology, I referred back to the three forms of state governance discussed in Chapter 2: democratic, hybrid, and authoritarian.

10.1.2.1 Democratic-Digital Hybrid Regime (D-DHR)

My study ascertained that there is no single definition or type of democracy in the literature. The same can be said for digital governance in democracies - there is no single definition or one type of digital governance that is used by all democracies. However, unlike scholarship focusing on different types of state democracies, the literature on digital democracy is limited and lacks consideration of associating different forms of digital governance with democratic states. My thesis fills this gap in the literature and argues that democratic states can have other types of digital governance that differ from digital democracies. To provide an example within the context of my thesis, I introduce the concept of a democratic-digital hybrid regime.

A democratic-digital hybrid regime (D-DHR) is one whose government practices strong democracy at the state level but has a hybrid digital governance regime online. As discussed in Section 2.1, strong democracies are associated not only

with their protection and preservation of fundamental individual rights, but also with protecting this in practice and in the government's functioning (Schmitter and Karl, 1991; Dahl, 2000). Although non-democratic aspects depend on the context of the D-DHR country, one example of this could be protecting its citizens' life and liberty as core elements, while the rights to privacy, freedom of expression and speech, and access to information are diminished online. When compared to the hybrid-digital form of state governance (which will be discussed next), D-DHR may demonstrate stronger democratic principles in its digital governance due to its robust democratic state and its workings, like rule making and regulation, which affect its digital governance.

It is important to note that a D-DHR acts as the umbrella concept for any digitally hybrid democracy. Considering that democracies vary in type - direct, representative, deliberative, and constitutional (Linz, 2000; Held, 2006; Wessels, 2018) - I argue that there is no single type of D-DHR. Thus, the three constituent aspects of digital hybrid regimes lead to the creation of different sub-types of D-DHR, depending on the existing hybrid elements in a specific country. In sum, this subsection has demonstrated that strong democracies can have different forms and degrees of digital hybrid governance, like a D-DHR, where a strong state has a minimum protection of democratic principles but mass diminishments at digital levels.

10.1.2.2 Hybrid-Digital Hybrid Regime (H-DHR or 'full-scale hybrid regime')

As mentioned previously, hybrid states have been studied by scholars from both democratic and authoritarian fields, which is why there was a wide range of hybrid definitions in the literature. However, instead of approaching hybrid regimes as being inherently democratic or authoritarian¹¹⁹, I followed Gilbert and Mohseni's (2011) approach to hybrid regimes and applied this to the notion of a digital hybrid regime in hybrid states.

¹¹⁹ See Section 10.1.1.

By a hybrid-digital hybrid regime (H-DHR), I mean states with a hybrid political regime which also have a form of digital hybridity in their digital governance. As this is the same sort of regime at state and digital levels, I call these full-scale digital hybrid regimes. According to Gilbert and Mohseni (2011), the confusion among democratic and authoritarian scholars' approaches to hybrid regimes is due to hybrid states - unlike authoritarian ones - having elections and being multi-party systems, but simultaneously and in contrast to democracies, they have diminished forms of democratic regimes (Gilbert and Mohseni, 2011, pp. 273-4). In light of their empirical study on re-categorising hybrid regimes through competitiveness during elections, protection of civil liberties, and tutelary institutions (Gilbert and Mohseni, 2011, pp. 284-292), I assert that an H-DHR is where a country holds all or some of these three characteristics as part of their state governance¹²⁰, but also has a digital hybrid regime in terms of their digital governance. For example, it could be a state where elections are held but civil liberties are limited, whilst containing several digital elements of the operational, legal, or observed implications on the public aspects I have outlined in the previous section. Although hybrid elements at both state and digital levels depend on the context of the country studied, it can be said that H-DHR holds more of an authoritarian tendency and less democratic protection when compared to D-DHR, due to hybridity at the state governance level and its potential influence on the digital.

Like democracies, there was no single definition of types of hybrid regime in the literature. This could be seen not only from different scholars' approaches to democracies and authoritarianism, but also in Gilbert and Mohseni's (2011) categorisation of empirical findings into forms like illiberal hybrid regimes, illiberal tutelary hybrid regimes, or tutelary hybrid regimes. What emerged from this was that sub-types of H-DHR may vary not only at state levels, but also in their digital hybrid regimes. Instead of associating hybrid countries with digital democracies or digital authoritarianism, this type has described an alternative

¹²⁰ They created different types of hybrid regimes based on these three characteristics, which are discussed in the following paragraph.

digital regime for hybrid states and exposed a unique, full-scale form of hybrid governance.

10.1.2.3 Authoritarian-Digital Hybrid Regime (A-DHR)

Like the previously described regimes, there was no single definition and form of authoritarianism in the literature. Similar to democracies, the literature illustrated a gap in considering different forms of digital governance that authoritarian regimes can establish online. Therefore, by introducing the concept of an authoritarian-digital hybrid regime, this subsection not only contributes to the typology of digital hybrid regimes but also provides a definition of an alternative form of digital governance for authoritarian states.

By authoritarian-digital hybrid regimes (A-DHR), I mean countries with an authoritarian state regime that have digital hybrid governance. It is worth clarifying that the concept of authoritarianism has changed following the end of the Cold War, and some democratic elements have been integrated into it. Although some scholars view this type of authoritarian state as a hybrid form of governance, like Levitsky and Way (2002) and Diamond (2002), others consider the adaptation of authoritarianism into political systems' changing dynamics, like Brownlee (2007), and use of institutional democracy to protect a regime and balance social demands, like Brancati (2014) (see Section 2.2). What emerges from this is that an A-DHR is a state where an authoritarian regime is practiced, whether having democratic institutions or not, one that holds all or most of the elements of the three digital hybrid regime aspects described in the previous section (10.1.1.2). It is important to note that some scholars might confuse these institutional practices with hybrid regimes, as can be seen in Wright (2019)'s categorisation of Russia, which demonstrates an example of an A-DHR where Russia uses its democratic institutions to protect its authoritarian regime at state level, and practices a mixed regime online¹²¹. Although my thesis focuses on democracies, this nuanced evaluation proposes an interesting topic for further studies. Due to state governments' influence on establishing digital

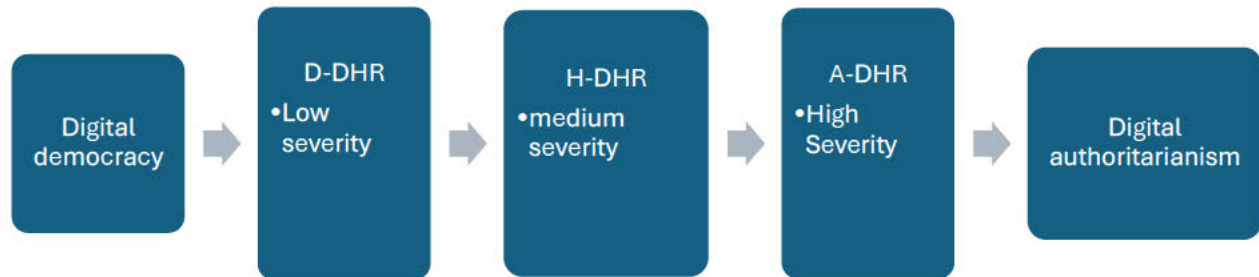
¹²¹ See Subsection 2.2.1 for digital authoritarian practices in Russia.

governance, an A-DHR would be more likely to have authoritarian-like aspects and minimum democratic elements than a D-DHR or an H-DHR.

An authoritarian-digital hybrid regime can be seen as the comprehensive concept for states which have authoritarian governance but contain hybrid features in their digital governance. Considering the multiple types of authoritarianism listed in Section 2.2, I argue that there can be different types of A-DHR due to variations in state forms and which aspects they have in their digital governance. In this thesis I suggest that authoritarian regimes are not limited to having digital authoritarianism as their digital governance, like Russia's digital governance which is predominantly classified as authoritarian (except by scholars like Wright 2019, see Subsection 2.2.1). The A-DHR is the last type of digital hybrid regime I have created in my research.

In summary, this section has set out a typology of digital hybrid regimes which I created from my study findings. Drawing on democratic, hybrid, and authoritarian states, it has not only expanded on my previous point about state versus digital governance but also demonstrated how the same digital governance regime can be adapted in different states. This reveals that, despite having a digital hybrid regime in common, different kinds of state regimes can influence the severity of hybrid regimes on digital governance. This can be explained due to each state's role in shaping digital governance, especially through laws, regulations, and control over multi-stakeholders in the digital sphere. Based on the above typology, I argue that the least severe type of digital hybrid regime is the D-DHR, followed by the H-DHR, and the most severe is the A-DHR. To illustrate these hybrid regimes' closeness to digital democratic and authoritarian forms of governance, I have produced Figure 10.1 below:

Figure 10.1: Severity of digital hybrid regimes



In short, digital hybrid regimes vary in type, not only due to their digital aspects, but also as a result of state regimes which shape every country's digital governance. This typology contributes to the digital governance literature and creates new areas for researchers to expand on and test on from interdisciplinary fields. Building on this innovative typology, the next section assigns types of digital hybrid regimes to India and the UK.

10.1.3 Digital Hybrid Regimes in India and the UK

Based on the above description and my research findings set out in Chapters 6 to 8, I categorise India as a 'full-scale digital hybrid regime' and the UK as a 'democratic-digital hybrid regime'. This is because, although they are both digitally hybrid, the severity of their hybridity differs in relation to their state governance and its implications on the digital aspects. To describe and highlight their differences, I discuss their prevailing hybrid characteristics through the framework I have devised, described in Section 10.1.1 above.

India's full-scale digital hybrid regime points out the importance of state governance in the digital sphere. From the operational aspect, India's government has not only developed and used tools itself, but has also purchased tools and collaborated with external firms, including SMPs. The hybridity element of this aspect emerged from my examination of the way it is used in India. As my findings show, India not only operates in a socially constructed way

at the national level¹²², but also protects its regime by monitoring key opposition figures, removing pieces of content that are not in the regime's interest, and spreading pro-regime-related content online¹²³. From the legal point of view, in my research I observed the dual usability of the law element in several instances in India. For instance, the law was used as a legitimising tool by the Ministry of Home Affairs when it was questioned in parliament about using Pegasus spyware. Another example was not just the infringement of individual rights, but also the use of terror laws to jail a journalist who had criticised the government. Furthermore, regarding the observed implications on the public aspect, my respondents from India highlighted not only common impacts of the government's actions on the public, like the lack of transparency or refusal of RTI requests, but also through India's inadequacy to control the digital governance of SMPs, as demonstrated widely in reported incidents of the killing of innocent people due to disinformation¹²⁴. That is not to say that India's discourse management is underdeveloped, however, what emerged from my findings is the fact that it is highly politicised and focused on the regime's survival in a way that de-prioritises ensuring the safe control of SMPs. Thus, this politicised motive not only demonstrates a core factor of its hybridity but also underscores the targeted impacts on socio-political groups observed in India. Considering the extreme outcomes like murders and arrests that result from India's digital governance management not only clarifies its difference from the UK but also exemplifies its H-DHR form of governance.

The UK's democratic-digital hybrid regime demonstrates stronger democratic practices and less authoritarian elements in its form. From the operational aspect, its hybridity can be seen not only in the technical operations and collaborations developed and implemented with external actors, but also in its police and military operations online¹²⁵. This integration of state forces into digital governance demonstrates a harsher regime in the UK than in India. However, it is noteworthy that the operations identified in the UK are conducted on a larger scale and are not targeted socio-politically on people who oppose the

¹²² Like technical -veillance programmes post-Mumbai attack, see Subsection 6.1.1.1.

¹²³ See sections on 'India' in Parts 1, 3, and 4 of Chapters 6, 7, and 8.

¹²⁴ See sections on 'India' in Parts 3 and 4 of Chapters 6, 7, and 8.

¹²⁵ See sections on 'United Kingdom' in Parts 1, 3, and 4 of Chapters 6, 7, and 8.

government. Additionally, in cases where these operations were seen as a scandal, like Cambridge Analytica's interference in elections, the UK demonstrated a more functioning democracy by not just questioning people in parliament, but also tackling the issues through laws and departmental working documents¹²⁶. From the legal aspect, the UK's D-DHR was shown to be infringing individual rights online, as it provides qualified rights. However, it also demonstrated stronger democratic practice, such as by preventing passing the 'legal but harmful' provision in the draft Online Safety Act. Hence, despite its non-democratic protection of individual rights, the UK's democratic state governance prevents more authoritarian outcomes of its legal aspect as part of its D-DHR. Regarding implications on the public aspect, the most prevailing observation among my respondents with regard to hybridity was the normalisation of non-democratic implications in the UK. Despite some campaigns aiming to increase public digital literacy, the UK public was believed by some respondents to have a general distrust regarding its digital governance, due to scandals and leaks.

Overall, this concludes my categorisation of India's H-DHR and the UK's D-DHR. Although one could argue that there are some interlinkages between the two countries, it is important to consider the difference in severity of their regimes discussed above, and their contextual differences outlined in Chapter 3. Thus, this section has demonstrated that, despite both countries having a formal democratic system of governance at the state level, their democracies in action have influenced the type of digital hybrid regimes constructed online, when governing SMPs. This underscores the importance of taking a comprehensive approach to understanding the complex dynamics of digital governance.

¹²⁶ See sections on 'United Kingdom' in Parts 3 and 4 of Chapters 6, 7, and 8.

10.2 Research Reflections

10.2.1 Contributions

My thesis makes four key contributions to the existing studies on digital governance - methodological, empirical, theoretical, and conceptual. The first contribution is methodological. Keeping in mind the complexity, timeliness, and interdisciplinarity of the research topic, I developed my own methodological approach to study digital governance. I started by taking an inductive approach and formulated an exploratory standpoint, which led to the search for, and then creation of, my qualitatively driven multimethod approach. My research used both qualitative and quantitative data, entailing a rich use of materials. By data collecting in a sequential order, I remained reflexive throughout all three stages, which helped me to narrow the focus of my exploratory research and make informed methodological choices at the end of each stage. This approach resulted in a distinctive, innovative methodological design, which enabled my research to stay on topic while covering the comprehensive aspects of digital governance. Thus, this confirms that my methodological approach is one of my research contributions to the field of interdisciplinary studies and sets out an example of studying the complexities of digital governance.

The second contribution of my research is the themes and aspects generated when exploring the digital governance of social media platforms in India and the UK. By employing a thematic analysis of the data collected, my research generated three themes: -veillance, content control, and shaped discourse. As discussed in Chapters 6 to 8, these themes enabled me to study both countries' digital governance of social media platforms through digital dual-use operations, the role of SMPs, legal frameworks, and observed implications on the public. Following the discussion provided in Chapter 9 in light of my SRQs, I outlined the constituent parts of the empirical perspective as operational, legal frameworks, and observed implications on the public. This means that my themes and digital governance aspects can be used as a framework in the fields of interdisciplinary studies and for those who want to explore digital governance research of social media platforms in other countries. Thus, this contribution can be transferrable

to different case studies or act as a starting point to be expanded or re-categorised in further research.

The third contribution of my research is theoretical. Following Anthony Giddens' theory of structuration, and its integration into technology by Jane Orlikowski and organisations by Geoff Walsham, I adopted structuration as the theoretical framework of my research and took a holistic approach to studying digital governance. This led to the creation of my 'structuration model of digital governance', described in Chapter 4, which enabled my research to focus on the interplay of structure, agent/agency, and technology in constantly shaping and co-constructing the digital governance of SMPs. Based on my reflections on my findings, given in Chapter 9, this theoretical model offers an alternative for interdisciplinary fields as it provides a comprehensive framework with which to study complex systems, like the digital governance of SMPs.

The final - and main - contribution of my research is conceptual. As detailed in the first part of this chapter, my thesis conceptualises digital hybrid regimes. Instead of mixing a state regime with its digital governance to create a digital hybrid regime (as proposed by Wright, 2019), my research perceives digital governance as a separate form of governance. This is due to the contextual characteristics of the digital sphere which differ from state governance, such as having multiple stakeholders online. Building on the literature and my empirical structuring of digital governance, I first explained this innovative concept and then generated three types of it, demonstrating its use in different state regimes. In doing so I have shown that digital hybrid regimes, as a form of digital governance, can be adopted by states which are democratic, hybrid, or authoritarian. This conceptual contribution not only introduces the need to approach state and digital regimes as two distinct levels of governance but also points out the different regimes that states can establish online, compared to their government in real life. Challenging the literature, I have demonstrated that a country's digital governance regime may not be the same as its state governance regime. This contribution is important because it not only introduces the digital concept of hybrid governance but also provides an original approach for interdisciplinary studies that can address state and digital governance.

In summary, my thesis makes four critical contributions to the emerging interdisciplinary field of digital governance. These not only generate room for further research and testing of the findings reported in my thesis, but also point out the gap left in the research (which is discussed more in Section 10.2.4 below).

10.2.2 Policy Recommendations for Digital Governance

A digital hybrid regime is a form of digital governance that sits in the grey area between digital democracies and digital authoritarianism. To reduce the risk of misusing digital dual-use operations, prevent digitally authoritarian practices, and strengthen digital democracy, this thesis outlines three policy recommendations for states' digital governance. It is important to clarify that these policy implications may not be limited to SMPs but could help enhance digital democracy at the level of digital governance as a whole.

The first recommendation is to understand the dual usability of operations and the importance of policies around them, as discussed in relation to my findings on -veillance, content control, and shaped discourse. One of the key suggestions that emerged from my case studies is the need to focus on policies around controlling these dual-usable operations. This can be enhanced by advancing democracy-centred policies on data collection and monitoring (-veillance, see Chapter 6), information controls (content control, Chapter 7), and manipulative or targeted discourse (shaped discourse, Chapter 8) on social media platforms. Policies around these themes would not only strengthen the democratic application of operations and control over SMPs but might also have a positive influence on election processes, the practicing of individual rights, and creation of a safer digital sphere.

The second recommendation is the need to re-evaluate state policies around regulating stakeholders online. This is not to limit the liberal features of democracies, but to ensure the objective regulation of diverse firms online. By firms, I refer to those multi-stakeholder companies that play a part in digital governance, including social media platforms, intermediaries that work on those platforms, and firms that sell and employ tools on social media platforms.

Moreover, my research findings show that India and the UK have different methods of engaging with private firms, which has led to many uncertainties and conspiracy theories about those who work in related digital governance fields¹²⁷. These shared concerns and viewpoints raise the importance of transparency between states and those firms. This reveals that states would not only benefit from enhancing their policies around regulating multi-stakeholders as part of their digital governance, but also that establishing a transparent engagement mechanism can help to enhance their digital democratic practices online.

The third recommendation is the need to take a citizen-centric approach in digital governance. Although the primary unit is the same in both states and social media platforms, my findings show that individual rights are being requisitioned by both platforms and states when it comes to digital governance. These include, but are not limited to, the rights to privacy, freedom of expression, freedom of speech, to make decisions without interference, and to receive and impart accurate information¹²⁸. My findings confirm the need to re-assert and centralise the individual in the digital governance agenda, for a stronger digital democracy. While policy makers can focus on advancing the state side of it, they can also use regulations to control and ensure that private firms adopt, respect, and are responsible for not breaching users' democracy. That is, instead of having policies that undermine democracy at the individual level, there is a need for policies which centralise preservation and protection at the lowest state unit, the individual.

These three recommendations advocate that states should prioritise following a democratic approach, not only in the processing of functioning government or law-making, but also in their practical implementation. Once again, although my research focused primarily on the digital governance of SMPs, these recommendations can be interpreted in relation to digital governance as building blocks.

¹²⁷ See Sections 6.1.2, 7.1.2, and 8.1.2.

¹²⁸ See Chapters 6, 7, and 8.

10.2.3 Limitations

There are three limitations to my research. The first is the generalisability of my case study design. As detailed in Chapter 5, I referred to my case selections as building blocks in studying digital governance. My findings contribute to this newly emerging interdisciplinary field but are limited to the contexts of India and the UK. Although my contributions can be applied, tested, and expanded on in further studies, it is essential to take into account the contextual bases of my case study countries, and the period when I was conducting this research. This not only included their social and political contexts, but also the timing of the global COVID-19 pandemic, which affected my research. Thus, although my research findings can be developed and further studied, it is essential to consider contextual circumstances as a potential limitation of their generalisability and transferability.

The second limitation is the number of interview respondents. Although my research obtained rich data from the 22 interviews conducted in Stage 2, the initial plan was to carry out 30 interviews. Instead of delaying the research process to complete all 30, I prioritised data saturation and the quality of the collected interview data. As explained in Chapter 5, the low turnout was a result of the COVID-19 pandemic and the timeliness of my research into somewhat sensitive topics, like political, social, cultural, and religious issues. As stated above, despite this limitation the 22 interviews provided rich data, from which I derived valuable insights.

The final limitation is the timeliness of my research topic. Although its timeliness is one of the factors that raises the importance of my thesis in contemporary studies, I encountered many changes during my research. As explained in Chapter 5, my research consisted of three stages of data collection, and I encountered some changes and developments between phases. These included the Online Safety Bill coming into law in the UK and Twitter's name being changed to X, among other things noted in my thesis. To mitigate this limitation, I conducted validation in Stage 3 and have detailed these changes throughout my thesis using footnotes, whilst keeping the original data to show the process of how democracies transform. Although this limitation challenged

me during my thesis writing process, it once again showed the evident importance and timeliness of my research topic.

10.2.4 Recommendations for Further Studies

Building on the previous sections on my research contributions and limitations, this thesis provides three recommendations for future research. The first recommendation is for scholars who align with my ontological and epistemological stance to use my approach to compare different regimes at state or digital levels, thereby enriching the field of digital governance. In this way, the methodological approach that I used in this study can assist researchers with their research models.

The second recommendation is to use, expand, or adapt the structuration model of digital governance developed in this thesis. Although my research specifically focused on SMPs, the framework can be integrated to other studies focusing on different multi-stakeholders in the digital sphere, enabling a holistic understanding of digital governance. As a new framework, the model demonstrates great promise for expansion and provides a flexible alternative for studying digital governance from interdisciplinary fields.

The final recommendation is to focus on the digital hybrid regime as an emerging subject area that is very timely and interdisciplinary. Considering its connection with the democratic and authoritarian literature, as well as its links to state-governance, it provides a new field that can be studied in social sciences. Overall, these proposed avenues for further studies show possible pathways to enhance our understanding of digital regimes and their implications for societies.

10.3 Concluding Remarks

Studying how India and the United Kingdom have constructed their digital governance on SMPs, by specifically focusing on Facebook and Twitter, has revealed the dynamic and interconnected nature of the digital sphere that is

constantly being (co-)constructed. As the previous chapters have detailed, this required a comprehensive examination of the digital governance of SMPs, which was found to comprise operational, legal, and observed implications on the public aspects. Despite comparing democratic countries from different regions and contexts, this research found that India and the UK had the same form of digital governance of SMPs, a digital hybrid regime. In my thesis I have defined a digital hybrid regime as **a unique form of digital governance that has a mixture of digital democratic and digital authoritarian elements**. Despite acknowledging the influence of states' governance on their digital hybrid regimes, I have distinguished state governance from digital governance, arguing that the state's influence only partially impacts digital governance, due to other multi-stakeholders online. Through this differentiation, this thesis has not only provided an alternative approach to studying digital governance but also exemplified that two countries with democratic state governance both have a digital hybrid regime on SMPs.

Starting from Chapter 1, this thesis has focused on the significance of SMPs, the dynamics of digital dual-use operations, the ambiguities surrounding their interpreted uses, the role of multi-stakeholders in the digital sphere, and states' expanding governance over these domains. Chapters 2, 3, 6, 7, and 8 highlighted the importance of contextual differences in shaping how digital governance is constructed, including the socio-political and legal contexts. Chapter 4 outlined my normative liberal internationalist position and introduced the structuration model of digital governance I developed for this research. Chapter 5 detailed my research methodology and approach that generated the empirical findings presented in Chapters 6 to 8 on digital dual-use operations, the role of SMPs, the legal frameworks, and experts' concerns about impact on the public in India and the UK. Chapter 9 then synthesised the thematic findings in relation to my research questions and compared both countries. This comparison produced empirical and theoretical perspectives and informed the 'digital hybrid regimes' concept, which was further developed in this chapter. After ten chapters of detailed discussion and examination, this concludes my timely and interdisciplinary thesis on how India and the UK construct their digital

governance in relation to *SMPs* and their broader significance for democracies and digital governance.

Appendices

Appendix 1: Freedom in the World (2020-2022)

	INDIA			UNITED KINGDOM (UK)		
	2020	2021	2022	2020	2021	2022
Freedom Score	71/100 Free	67/100 Partly Free	66/100 Partly Free	94/100 Free	93/100 Free	93/100 Free
Political Rights	34/40	34/40	33/40	39/40	39/40	39/40
Civil Liberties	37/60	33/60	33/60	55/60	54/60	54/60

	INDIA			UK		
	2020	2021	2022	2020	2021	2022
A- Electoral Process (Political Rights)						
A.1: Was the current head of government or other chief national authority elected through free and fair elections?	4/4	4/4	4/4	4/4	4/4	4/4
A.2: Were the current legislative representatives elected through free and fair elections?	4/4	4/4	4/4	4/4	4/4	4/4
A.3: Are the electoral laws and framework fair, and are they implemented impartially by the relevant election management bodies?	4/4	4/4	4/4	4/4	4/4	4/4
B- Political Pluralism and Participation						
B.1: Do the people have the right to organise in different political parties or other competitive political groupings of their choice, and is the system free of undue obstacles to the rise and fall of these competing parties or groupings?	4/4	4/4	3/4	4/4	4/4	4/4
B.2: Is there realistic opportunity for the opposition to increase its support or gain power through election?	4/4	4/4	4/4	4/4	4/4	4/4
B.3: Are the people's political choices free from domination by the military, foreign powers, religious hierarchies, economic	3/4	3/4	3/4	4/4	4/4	4/4

oligarchies, or any other powerful group that is not democratically accountable?						
B.4: Do various segments of the population (including ethnic, religious, gender, LGBT, and other relevant groups) have full political rights and electoral opportunities?	2/4	2/4	2/4	4/4	4/4	4/4
C- Functioning of Government						
C.1: Do the freely elected head of government and national legislative representatives determine the policies of the government?	4/4	4/4	4/4	3/4	4/4	4/4
C.2: Are safeguards against official corruption strong and effective?	2/4	2/4	2/4	4/4	3/4	3/4
C.3: Does the government operate with openness and transparency?	3/4	3/4	3/4	4/4	4/4	4/4
D- Freedom of Expression and Belief (Civil Liberties)						
D.1: Are there free and independent media?	2/4	2/4	2/4	4/4	4/4	4/4
D.2: Are individuals free to practice and express their religious faith or nonbelief in public and private?	2/4	2/4	2/4	4/4	4/4	4/4
D.3: Is there academic freedom, and is the educational system free from extensive political indoctrination?	2/4	2/4	2/4	3/4	3/4	3/4
D.4: Are individuals free to express their personal views on political or other sensitive topics without fear of surveillance or retribution?	4/4	3/4	3/4	3/4	3/4	3/4
E- Associational and organisational rights						
E.1: Is there freedom of assembly?	2/4	2/4	2/4	4/4	4/4	4/4
E.2: Is there freedom for nongovernmental organisations, particularly those that are engaged in human rights- and governance-related work?	3/4	2/4	2/4	4/4	4/4	4/4
E.3: Is there freedom for trade unions and similar professional or labor organisations?	3/4	3/4	3/4	4/4	4/4	4/4
F- Rule of Law						
F.1: Is there an independent judiciary?	3/4	2/4	2/4	4/4	4/4	4/4
F.2: Does due process prevail in civil and criminal matters?	2/4	2/4	2/4	4/4	3/4	3/4
F.3: Is there protection from the illegitimate use of physical force and freedom from war and insurgencies?	2/4	2/4	2/4	3/4	3/4	3/4

F.4: Do laws, policies, and practices guarantee equal treatment of various segments of the population?	2/4	2/4	2/4	3/4	3/4	3/4
G- Personal Autonomy and Individual Rights						
G.1: Do individuals enjoy freedom of movement, including the ability to change their place of residence, employment, or education?	3/4	2/4	2/4	4/4	4/4	4/4
G.2: Are individuals able to exercise the right to own property and establish private businesses without undue interference from state or nonstate actors?	3/4	3/4	3/4	4/4	4/4	4/4
G.3: Do individuals enjoy personal social freedoms, including choice of marriage partner and size of family, protection from domestic violence, and control over appearance?	2/4	2/4	2/4	4/4	4/4	4/4
G.4: Do individuals enjoy equality of opportunity and freedom from economic exploitation?	2/4	2/4	2/4	3/4	3/4	3/4

Appendix 2: Freedom on the Net (2019-2021)

	INDIA			UNITED KINGDOM (UK)		
	2019	2020	2021	2019	2020	2021
Freedom Score	55/100 Partly Free	51/100 Partly Free	49/100 Partly Free	77/100 Free	78/100 Free	78/100 Free
Obstacles to Access	12/35	12/25	11/25	22/25	23/25	23/25
Limits on Content	24/35	21/35	32/35	30/35	30/35	30/35
Violations of User Rights	19/40	18/40	12/40	25/40	25/40	25/40

	INDIA			UK		
	2019	2020	2021	2019	2020	2021
A- Obstacles to Access						
A.1: Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	3/6	3/6	3/6	6/6	6/6	6/6
A.2: Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	1/3	1/3	1/3	2/3	2/3	2/3
A.3: Does the government exercise technical or legal control over internet infrastructure for the purpose of restricting connectivity?	2/6	2/6	1/6	5/6	6/6	6/6
A.4: Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	4/6	4/6	4/6	5/6	5/6	5/6
A.5: Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	2/4	2/4	2/4	4/4	4/4	4/4
B- Limits on Content						
B.1: Does the state block or filter, or compel service providers to block or filter, internet content?	3/6	3/6	3/6	5/6	5/6	5/6

B.2: Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete the content?	3/4	2/4	2/4	3/4	3/4	3/4
B.3: Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	2/4	2/4	2/4	3/4	3/4	3/4
B.4: Do online journalists, commentators, and ordinary users practice self-censorship?	3/4	3/4	3/4	3/4	3/4	3/4
B.5: Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	2/4	2/4	2/4	3/4	3/4	3/4
B.6: Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	3/3	2/3	2/3	3/3	3/3	3/3
B.7: Does the online information landscape lack diversity?	3/4	3/4	3/4	4/4	4/4	4/4
B.8: Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	5/6	4/6	4/6	6/6	6/6	6/6
C- Violations of User Rights						
C.1: Do the constitution or other law firms fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that independence?	4/6	4/6	4/6	5/6	5/6	5/6
C.2: Are there laws that assign criminal penalties or civil liability for online activities?	2/4	2/4	2/4	2/4	2/4	2/4
C.3: Are individuals penalized for online activities?	2/6	2/6	2/6	5/6	5/6	5/6
C.4: Does the government place restrictions on anonymous communication or encryption?	3/4	3/4	2/4	2/4	2/4	2/4
C.5: Does the state surveillance of internet activities infringe on users' right to privacy?	2/6	1/6	1/6	2/6	2/6	2/6
C.6: Are service providers and other technology companies required to aid	2/6	2/6	2/6	3/6	3/6	3/6

the government in monitoring the communications of their users?						
C.7: Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	2/5	2/5	2/5	4/5	4/5	4/5
C.8: Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattacks?	2/3	2/3	2/3	2/3	2/3	2/3

Appendix 3: FoN Reports' Codes and Themes

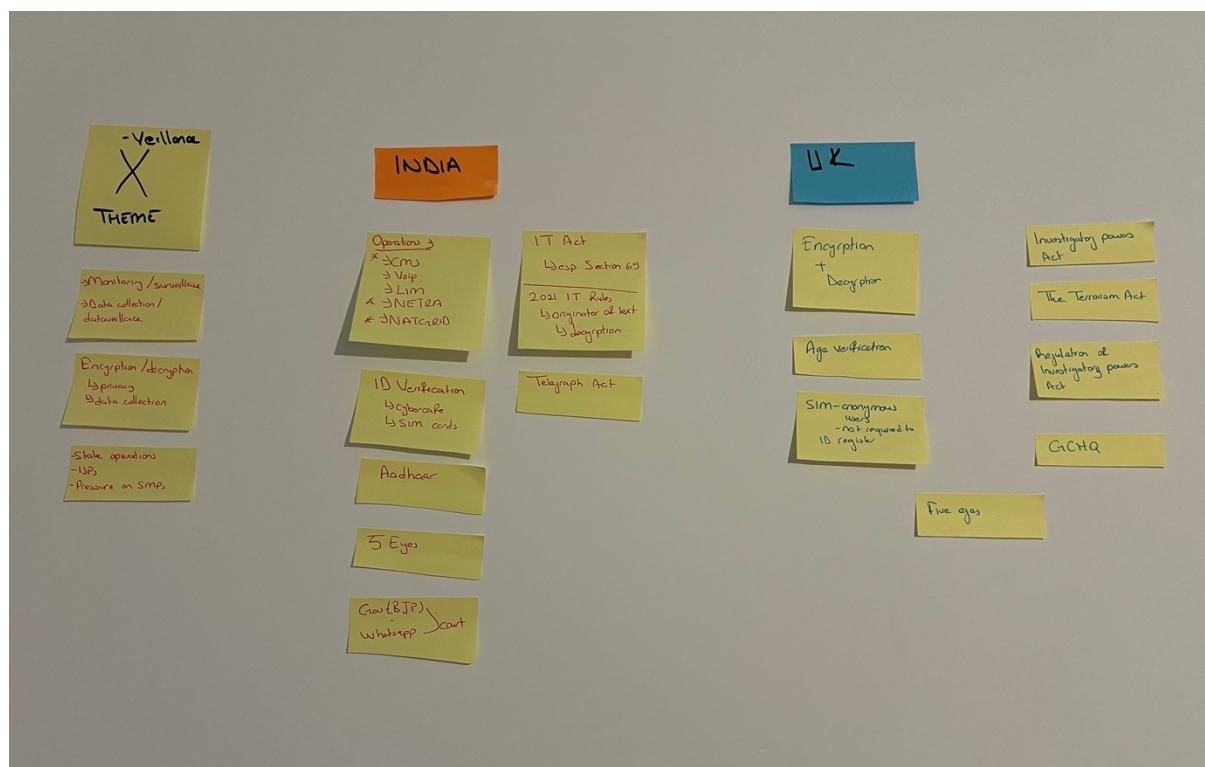
Theme 1: Internet Disruption



Theme 2: Content Control



Theme 3: -Veillance



Appendix 4: Legal Extracts and Notes

4.1 The Universal Declaration of Human Rights (1948)

The Universal Declaration of Human Rights is an international declaration published by the United Nations in 1948. It acts as a universal guideline that lists individual rights and freedoms. Although it has no legal obligation, it plays an ideal role for countries and is an example for liberal internationalism. In this thesis, I have referred to the following articles:

- **Article 12:** No one shall be subjected to arbitrary interference with his [sic] privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (Universal Declaration of Human Rights, 1948).
- **Article 18:** Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his [sic] religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance (ibid.).
- **Article 19:** Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers (ibid.).

4.2 Indian Legislation

The Indian Constitution (1950)

The Constitution of India is the supreme law of the country. It establishes the political system of the state, defines the powers of its institutions, and guarantees fundamental rights of its citizens. In this thesis, I primarily drew on the following articles:

- **Article 19.1.a:** ‘All citizens shall have the right to freedom of speech and expression’ (The Indian Constitution, 1950).

- **Article 21:** ‘Protection of life and personal liberty. —No person shall be deprived of his life or personal liberty except according to procedure established by law’ (ibid.).
- **Article 25:** (2) Nothing in this article shall affect the operation of any existing law or prevent the State from making any law— (a) regulating or restricting any economic, financial, political or other secular activity which may be associated with religious practice; (b) providing for social welfare and reform or the throwing open of Hindu religious institutions of a public character to all classes and sections of Hindus (ibid.).
- **See Part III** of the Constitution for ‘Fundamental Rights’ (ibid.).
- **See Article 324** for ‘Superintendence, direction and control of elections to be vested in an Election Commission’ (ibid.).

The Indian Constitution (Sixteenth Amendment) Act (1963)

The Indian Constitution (Sixteenth Amendment) Act introduced new restrictions to freedom of speech and expression. This includes the ‘sovereignty and integrity of India’ as listed in Article 19.2:

- **Article 19.2:** Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of [the sovereignty and integrity of India - 1963 Amendment], the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence (The Indian Constitution (Sixteenth Amendment) Act, 1963).

The Right to Information Act (2005)

The Right to Information Act empowers citizens to request information from the government. In this thesis, I used this Act to contextualise dataveillance rights from the stance of agency and to point out its limited scope:

- **See Article 8** for the long list of ‘Exemptions from disclosure of information’ (The Right to Information Act, 2005).

The Indian Telegraph Act (1885)

The Indian Telegraph Act is legislation enacted during British colonial rule in India. It establishes a framework for controlling telegraphs and regulating communications. The Act continues to be implemented in India and has been expanded through subsequent allied rules (like the Indian Telegraph Rules, 1951) and newer legislation, the Telecommunications Act (2023). In this thesis, I drew mainly on Section 5 of the Act:

- Section 5: Power for Government to take possession of licensed telegraphs and to order interception of messages.** (1) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act. (2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this subsection (Indian Telegraph Act, 1885).

The Indian Telegraph Rules (1951)

The Indian Telegraph Rules (1951) were introduced as an extension of the Indian Telegraph Act (1885). They modernise the procedural aspects of interception, use of devices, and outline the protocol on government's access to communication. In this thesis, I referred to these Rules particularly in relation to the change in government interception procedures (see Subsection 6.3.1.2).

The Telecommunications Act (2023)

The Telecommunications Act came into force in December 2023. Its goal is to modernise the existing frameworks in regulating telecommunication services and interception. In validation of one of my respondent's concerns, I referred specifically to Sections 3 and 20 (see Subsection 6.3.1.2).

The Information Technology Act (2000)

The Information Technology Act (IT Act) is the primary legislation governing electronic records and digital interactions in India. While it remains in force, the IT Act has been expanded through several rules and amendments, including the Information Technology (Amendment) Act (2008), the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public Rules (2009), and The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. One of the most referenced provisions of the Act in my thesis is:

- **Sub-section 69.A:** (1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of the sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored, or hosted in any computer resource (Information Technology Act, 2000).

The Information Technology (Amendment) Act (2008)

The Information Technology (Amendment) Act revised the IT Act and expanded its provisions about cybersecurity. In this thesis, I referenced the following provision:

- **Sub-section 69.B:** ‘power authorised to monitor and collect traffic data or information through any computer resource for Cyber Security’ (Information Technology (Amendment) Act, 2008).

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules (2009)

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules are an allied set of Rules of the IT Act and are commonly referred to as the Blocking Rules. It is a key legislation governing the blocking of online content. In my thesis, I referenced the following provisions:

- **See Rule 7** for ‘Committee for examination of the request’ (Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009).
- **See Rule 8** for ‘Examination of the Request’ (ibid.).
- **Rule 16:** ‘Strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof’ (ibid.).

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021)

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules are another set of allied rules to the IT Act. They establish a significant legal mechanism for the regulation of intermediaries and digital platforms that have more than five million users, including social media platforms. In this thesis, I referred to the following provisions of the Rules:

- **Sub-clause 3.1.d:** [...] an intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of

court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force:

Provided that any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorized agency, as may be notified by the Appropriate Government:

Provided further that if any such information is hosted, stored or published, the intermediary shall remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be:

Provided also that the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act; [...] (The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021).

- **See Sub-clause 3.1.g** for data retention duration, 180 days (ibid.).
- **Sub-clause 3.1.j:** the intermediary shall, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorized for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents:

Provided that any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be (ibid.).

- **See Sub-clauses 4.a to 4.c** for the definitions of the duties of three officers in ‘Additional due diligence to be observed by significant social media intermediary [and online gaming intermediary]’ (ibid.).
- **See Sub-section 4.2** which allows authorities to request decryption for reasons including: ‘public order, sexually explicit or child abuse material, and India’s sovereignty, integrity, and security’ (ibid.).
- **Sub-section 4.4:** A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical

in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary (ibid.).

- **Section 7:** Where an intermediary fails to observe these rules, the provisions of sub-section (1) of the section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.

The Digital Data Protection Act (2023)

The Digital Data Protection Act is India's first legislation on personal data protection. It was developed by a committee established in 2018. The following provisions of the Act were referenced in this thesis:

- **See Section 3** for the definition of 'digital personal data' and its territorial availability (The Digital Personal Data Protection Act, 2023).
- **See Sub-section 11.1** regarding citizens' rights, it grants Data Principals (individuals whose data has been collected) the right to be descriptively informed about the processing of their data (ibid.).
- **See Sub-section 11.2** for the limitation of 11.1: 'purposes of prevention or detection on investigation of offences or cyber incidents, or for prosecution or punishment of offences' (ibid.).
- **See Section 16** for processing of data outside India, which can be controlled by the central government (ibid.).
- **See Chapter V** for 'Data Protection Board of India' and **Chapter VI** for 'Powers, Functions and Procedure to be followed by Board' (ibid.).

The Copyright Act (1957)

The Copyright Act is legislation that protects original works and their creators. The following Sections of the Act were referenced in this thesis:

- **See Section 51** for 'When copyright is infringed' and legal consideration to those who are unaware of infringement (The Copyright Act, 1957).

- **See Section 63**, which prohibits selling and spreading of copyright content under ‘Offence of infringement of copyright or other rights conferred by this Act’ (ibid.).

The Copyright (Amendment) Act (2012)

The Copyright (Amendment) Act is an amendment of the Copyright Act (1957). In this thesis, I referred the Act for expanding regulation into the digital sphere and for expanding responsibility to intermediaries for the technical protection of right holders (see Subsection 7.3.1.2).

The Indian Penal Code (1860)

The Indian Penal Code is a criminal code from the colonial era that is also applied to online communications. It outlines criminal offences and their punishment. In this thesis, I referred to Sections in the following Chapters of the Code:

- **See Chapter VI (Sections 121-130)** for ‘Of Offences Against the State’ (The Indian Penal Code, 1860).
- **See Chapter VIII (Sections 141-160)** for ‘Of Offences Against the Public Tranquillity’ (ibid.).
- **See Chapter XXI (Sections 499-502s)** for ‘Of Defamation’ (ibid.).
- **See Chapter XXII (Sections 503-510)** for ‘Of Criminal Intimidation, Insult and Annoyance’ (ibid.).

The Disaster Management Act (2005)

The Disaster Management Act provides the legal framework for preventing and managing disasters. In this thesis, the following Sections were referenced in relation to the COVID-19 pandemic:

- **Section 54:** Punishment for false warning - Whoever makes or circulates a false alarm or warning as to disaster or its severity or magnitude, leading

to panic, shall on conviction, be punishable with imprisonment which may extend to one year or with fine (The Disaster Management Act, 2005).

- **Section 67:** The National Authority, the State Authority, or a District Authority may recommend to the Government to give direction to any authority or person in control of any audio or audio-visual media or such other means of communications as may be available to carry any warning or advisories regarding any threatening disaster situation or disaster, and the said means of communication and media as designated shall comply with such direction (ibid.).

The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules (2017)

The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules (2017) provide a framework for the temporary shutdown of internet and telecom services during public emergencies to ensure public security. In this thesis, I referred to these Rules to contextualise the legal basis for internet restrictions in India (see Subsection 8.3.1.2).

4.3 UK legislation

The Human Rights Act (1998)

The Human Rights Act is the primary legislation listing fundamental rights and freedoms of individuals in the UK. It is the national legal incorporation of the European Convention on Human Rights. In this thesis, I referred to the following Articles of the Act:

- **Article 3 of Protocol No.1:** The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature (Schedule 1, the Human Rights Act, 1998).
- **Article 8.1:** Everyone has the right to respect for his [sic] private and family life, his home and his correspondence (ibid.).
- **Article 8.2:** There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is

necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (ibid.).

- **Article 9.1:** Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his [sic] religion or belief, in worship, teaching, practice and observance (ibid.).
- **Article 9.2:** Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others (ibid.).
- **Article 10.1:** Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises (ibid.).
- **Article 10.2:** The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary (ibid.).

The Freedom of Information Act (2000)

The Freedom of Information Act (FOIA) allows the public to request information from authorities in England, Wales, and Northern Ireland. In this thesis, I have referred to the FOIA to contextualise dataveillance rights in relation to the agency in the UK and highlight its limited scope under its 'Part II Exempt information' in Chapter 6.

The Freedom of Information (Scotland) Act (2002)

The Freedom of Information (Scotland) Act (FOISA) enables the public to request information from Scottish authorities. Like FOIA, I used FOISA to contextualise dataveillance rights in relation to the agency in the UK and noted its limited scope under ‘Part 2 Exempt Information’ in Chapter 6.

The Regulation of Investigatory Powers Act (2000)

The Regulation of Investigatory Powers Act establishes a framework for the lawful use of surveillance, interception, and investigatory powers in the UK. In this thesis, RIPA is referenced to contextualise the regulatory environment and its relevance to discussions on the Tempora programme revealed by Edward Snowden. The powers and duties outlined in this Act were later re-defined in the Investigatory Powers Act (2016).

The Investigatory Powers Act (2016)

The Investigatory Powers Act consolidates existing laws on interception, interference, and data retention. It was introduced following concerns regarding gaps identified in GCHQ’s practices (see Subsection 6.1.2.1). In this thesis, I referenced the following Sections of the Act:

- **Section 57** ‘prohibit[s] telecommunication providers from disclosing the existence of a warrant’ (Investigatory Powers Act, 2016)
- **Section 87** outlines its ‘powers to require data retention of certain data’, where Sub-section 87.1 states that the Secretary of State must issue any notice to a telecommunication operator (ibid.).
- **Sub-section 87.2:** ‘A retention notice may -
 - (a) relate to a particular operator or any description of operators,
 - (b) require the retention of all data or any description of data,
 - (c) identify the period or periods for which data is to be retained,
 - (d) contain other requirements, or restrictions, in relation to the retention of data,
 - (e) make different provision for different purposes,
 - (f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice (ibid.).

- **Sub-section 87.3** specifies that this must be ‘retained no more than 12 months’ (ibid.).
- **See Part 6** for bulk warrants (ibid.).
- **See Part 7** for data retention and examination of the data by intelligence services (ibid.).
- **See Part 8** for the oversight mechanism (ibid.).

The Data Protection Act (2018)

The Data Protection Act is the national implementation of the European Union’s General Data Protection Regulation. It defines individual rights over their personal data and sets out obligations for organisations in the processing of their data. In this thesis, I referred to the following provisions of the Act:

- **Sub-section 3.2:** “‘personal data’ means any information relating to an identified or identifiable living individual’ (The Data Protection Act, 2018).
- **Sub-section 3.3:** By ‘identifiable living individual’ the legislation covers not just the identity or credentials of individuals, but other specific characteristics that make it possible to identify them (ibid.).
- **See Sections 10 and 11** for special category of data (ibid.).
- **See Part 3-Chapter 3** for data subjects’ rights, like the right to rectification or erasure (Sections 46-48), ensuring some individual control over their data, but this may also conflict with provisions such as the special processing of data (ibid.).

The Digital Economy Act (2017)

Digital Economy Act is legislation for managing digital economy and public services, while protecting consumers online. I have referenced the following parts of the Act in this thesis:

- **See Part 3 (Sections 14 to 30)** for ‘Online Pornography’ (The Digital Economy Act, 2017).
- **See Section 32** for the amendments on the Copyright, Designs and Patents Act (1998) (ibid.).
- **Sub-section 104.1:** A provider of an internet access service to an end-user may prevent or restrict access on the service information, content, applications or services, for child protection or other purposes, if the action is in accordance with the terms on which the end-user uses the service (ibid.).

The Copyright, Designs and Patents Act (1988)

The Copyright, Designs and Patents Act is legislation that focuses on the protection of intellectual property. In this thesis, I referenced the following clause:

- **Section 97.A.1:** The High Court (on Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright (The Copyright, Designs and Patents Act, 1988)

The Terrorism Act (2006)

The Terrorism Act is legislation introduced to expand existing laws on terror. In this thesis, the following provision was referenced in relation to the publication of content that glorifies terrorism:

- **See Section 3** for actions related to terrorist content, including a notice and compliance (Terrorism Act, 2006).

The Online Safety Act (2023)

The Online Safety Act is legislation that was enacted in October 2023. It is centred on protecting users, especially children, from illegal content. It outlines duties for intermediaries, establishes an oversight mechanism, and enforces age-verification requirements. I have referenced the following sections in this thesis:

- **See Section 17** for the list on duties to protect ‘the free expression of content of democratic importance’ (Online Safety Act, 2023).
- **See Section 81.4** for ‘Duties about regulated provider pornographic content’ and the enforcement date of age verification, which is 17.1.2025 (ibid.).
- **See Subclauses 121.2.a.i to 121.2.a.iv** of use of ‘accredited technology’ for terrorist and child sexual exploitation and abuse content (ibid.).
- **See Part 7** for the Office of Communications (Ofcom) to regulate, ensure compliance, and issue fines or prosecution as an oversight mechanism of the service providers (ibid.).

Appendix 5: India-Facebook: Government Requests for User Data

India-Facebook (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July-Dec 2021
Total requests	22,684	26,698	35,560	40,300	45,275	50,382
Legal process requests	21,069	24,944	33,374	37,865	42,458	47,123
Emergency disclosure requests	1,615	1,754	2,186	2,435	2,817	3,259
Users/Accounts requested	33,324	39,664	57,294	62,754	68,485	81,501
% of data produced	54%	57%	50%	52%	51%	64%

Appendix 6: India-Twitter: Government Information Requests

India- Twitter (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July- Dec 2021
Information Requests (combined)	474	789	2,613	3,615	2,175	2,211
Routine	395	662	2,367	3,463	1,964	2,027
Emergency	79	127	246	152	211	184
Accounts Specified (combined)	1,268	2,873	6,346	7,762	7,959	7,768
Routine	1,162	2,683	5,906	7,508	7,287	7,492
Emergency	106	190	440	254	672	276
Compliance Rate (combined)	5%	1.6%	1%	0.6%	2.3%	5.5%
Routine	5.3%	1.8%	1%	0.6%	1.9%	5.6%
Emergency	3.8%	0.7%	0.8%	0.6%	5.6%	4.8%
Preservation requests	36	144	526	1,585	951	2,153
Accounts	145	1,028	2,366	3,877	5,865	9,852

Appendix 7: UK-Facebook: Government Requests for User Data

UK- Facebook (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July- Dec 2021
Total requests	7,721	8,378	9,185	10,526	10,678	10,117
Legal process requests	6,156	5,910	7,202	8,241	8,738	8,528
Emergency disclosure requests	1,565	2,468	1,983	2,285	1,940	1,589
Users/Accounts requested	10,550	9,885	10,819	12,753	12,728	12,001
% of data produced	90%	88%	88%	88%	88%	89%

Appendix 8: UK-Twitter: Government Information Requests

UK- Twitter (2019-21)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July-Dec 2021
Information Requests (combined)	658	433	487	470	470	456
Routine	358	320	380	375	402	383
Emergency	300	113	107	95	68	73
Accounts Specified (combined)	810	522	580	647	797	711
Routine	469	401	459	545	714	634
Emergency	341	121	121	102	83	77
Compliance Rate (combined)	67%	51.7%	42.7%	33.6%	38.3%	48.2%
Routine	62%	52.1%	43.6%	35.7%	38.8%	51.4%
Emergency	73%	50.4%	39.2%	25.2%	35.2%	31.5%
Preservation Requests (combined)	37	102	70	55	65	21
Accounts requested	91	56	92	81	227	109

Appendix 9: India-Facebook: Content Restrictions

(India-Facebook, n.d.-a)	Jan- June 2019	July- Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July-Dec 2021
Amount of Content Restricted						
Restricted in this country only	1.25k	841	824	932	535	369
Restrictions Applied to Others	0	0	0	0	0	0
Global Restriction Externally imposed	0	0	0	12	3	21
Restrictions by Products						
Album	0	0	0	0	0	0
Comment	1	0	0	0	0	0
Page and Group	19	79	104	104	66	74
Post	1.21k	691	465	322	219	245
Profile	2	11	81	100	91	3
Event*	-	-	-	0	0	0

Appendix 10: India-Twitter: Removal Requests

(India-Twitter, n.d.-b)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July- Dec 2021
Legal demands (combined)	504	782	2,772	6,971	4,903	3,992
Court orders	8	7	4	15	9	23
Other legal demands	496	775	2,768	6,956	4,894	3,969
Accounts Specified (combined)	2,484	7,834	13,200	19,128	17,125	12,916
Court orders		1,230	9	220	614	420
Other legal demands		6,604	13,191	18,908	16,511	12,496
Compliance rate (combined)	0%	36.7%	13.9%	9.1%	11.8%	19.5%
Court orders	-	85.7%	25%	73.3%	88.9%	69.6%
Other legal demands	-	36.3	13.8%	9%	11.7%	19.2%
Accounts TOS (combined)	578	992	1,159	1,310	1,319	1,585
Court orders	-	4	0	2	0	1
Other legal demands	-	988	1,159	1,308	1,319	1,584
Accounts withheld	73	16	17	60	1,300	88
Tweets withheld	241	1,481	377	598	446	303

Appendix 11: UK-Facebook: Content Restrictions

(UK-Facebook, n.d.-a)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July-Dec 2021
Amount of Content Restricted						
Restricted in this country only	76	231	3.63k	6.07k	1.35k	1.27k
Restrictions Applied to Others	0	0	0	0	0	0
Global Restriction Externally imposed	0	0	0	12	3	21
Restrictions by Products						
Album	0	0	1	9	0	2
Comment	6	2	6	10	0	0
Page and Group	5	31	38	61	85	50
Post	65	190	239	481	1.06k	752
Profile	0	5	2	5	0	3
Event*	-	-	-	7	3	1

Appendix 12: UK-Twitter: Removal Requests

(UK-Twitter, n.d.)	Jan-June 2019	July-Dec 2019	Jan-June 2020	July-Dec 2020	Jan-June 2021	July- Dec 2021
Legal demands (combined)	64	35	71	27	42	16
Court orders	0	9	14	6	6	4
Other legal demands	64	26	57	21	36	12
Accounts Specified (combined)	110	39	77	28	73	174
Court orders	-	13	16	6	47	129
Other legal demands	-	26	61	22	26	45
Compliance rate (combined)	0%	25.7%	32.4%	33.3%	35.7%	37.5%
Court orders	-	26.9%	71.4%	33.3%	33.3%	75%
Other legal demands	-	22.2%	22.8%	33.3%	36.1%	25%
Accounts TOS (combined)	39	10	20	8	22	19
Court orders	-	7	3	0	2	1
Other legal demands	-	3	17	8	20	18
Accounts withheld	0	0	0	0	0	2
Tweets withheld	0	13	699	155	0	5

Appendix 13: Participant Information Sheet

Participant Information Sheet



College of Social Sciences

Exploring digital authoritarianism in democracies through social media management.

Researcher: Seher Kurt, PhD student

Department: School of Social Sciences, University of Glasgow

Supervisors: Professor Bridgette Wessels, Professor Andrew Hoskins, and Professor Martin Kretschmer

You are being invited to take part in a research study. Before you decide to take part, it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully and discuss it with others if you wish. Ask the researcher if there is anything that is not clear or if you would like more information. Take some time to decide whether or not you wish to take part.

Thank you for reading this.

The purpose of this project is to understand the extent of digital authoritarianism in two democracies, India and the United Kingdom, by focusing on government management of social media platforms and its impact on individual rights between 2019-2021. This research explicitly focuses on social media platforms of Meta (Facebook) and Twitter. Your participation will support our work on understanding how digitally authoritarian democracies manage social media by focusing on its affect at individual-levels.

Participation in this study is voluntary. We chose to contact you and other potential participants based on works and activities related to digital sphere. Your participation to this research will involve a semi-structured online interview (approx. 45-60 min) and will be part of 30 interviews from India and the United Kingdom. We will conduct interviews remotely through Teams or Zoom. Although we prefer to have interviews on Teams as the University, we encourage you to choose and mention the one that is more comfortable and convenient for you on the consent form. We will store all your personal data securely on OneDrive and work on de-identified transcripts - to protect your personal information we will separate your personal data from research data- for reviewing, analysing, and studying during this research. Please note that the research data obtained from interviews may be used in journal articles, conference papers, presentations, other publications alongside with PhD thesis. We expect to complete this research project by 1st October 2023. Please be assured that we will delete all your personal data and the research data will be anonymous. However, please note that anonymity may not guarantee confidentiality due to the number of participants in this research. In such circumstances we might do additional removals on the research data to preserve your confidentiality. The

remainder research data will be submitted to the University's Enlighten for 10 years of retention.

This project has been considered and approved by the Research Ethics Committee of the College of Social Sciences, University of Glasgow.

For further information, please email Seher Kurt: [REDACTED]

To pursue any complaint about the conduct of the research: contact Lead for Ethical Review of College of Social Sciences, Dr Susan Batchelor, email:

[REDACTED] .

_____End of Participant Information Sheet_____

Appendix 14: Privacy Notice

Privacy Notice for Participation in Research Project: Exploring digital authoritarianism in democracies through social media management

Your Personal Data

The researcher and the University of Glasgow are the joint “Data Controllers” for your personal data collected during the study. This privacy notice will explain how the researcher and the University of Glasgow will process your personal data.

Why we need it

We are collecting basic personal data such as your name and contact details (email), recordings from interviews and, where relevant, limited special categories data (such as political views) to conduct our research. We need your name and contact details to allow us to arrange the study interviews. All other data are required for data analysis purposes.

Legal basis for processing your data

We must have a legal basis for processing all personal data. In this instance, the legal bases are:

For personal data: *Article 6(1)(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*

For special category data: *Article 9(2)(j) processing is necessary for archiving purpose in the public interest, scientific or historical research purposes or statistical purposes*

What we do with it and who we share it with

All the personal data you submit is processed by the researcher and staff at the University of Glasgow. No personal data will be shared with individuals out with the research team or with any third parties.

How long do we keep it for?

Your personal data will be retained by the University until the completion of the research study (October 2023), after which it will be securely deleted.

Anonymised interview transcripts will be retained for a period of ten years in line with the University of Glasgow research data management guidelines.

What are your rights?*

GDPR provides that individuals have certain rights including: to request access to, copies of and rectification or erasure of personal data and to object to processing. In addition, data subjects may also have the right to restrict the processing of the personal data and to data portability. You can request access to the information we process about you at any time.

If at any point you believe that the information we process relating to you is incorrect, you can request to see this information and may in some instances request to have it restricted, corrected, or erased. You may also have the right to object to the processing of data and the right to data portability.

*Please note that the ability to exercise these rights will vary and depend on the legal basis on which the processing is being carried out.

If you wish to exercise any of these rights, please submit your request via the [webform](#) or contact dp@gla.ac.uk

Complaints

If you wish to raise a complaint on how we have handled your personal data, you can contact the University Data Protection Officer who will investigate the matter. Our Data Protection Officer can be contacted at dataprotectionofficer@glasgow.ac.uk

If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law, you can complain to the Information Commissioner's Office (ICO) <https://ico.org.uk/>

Appendix 15: Consent Form



College of Social
Sciences

Consent Form

Title of Project: Exploring digital authoritarianism in democracies through social media management.

Name of Researcher: Seher Kurt

Name of Supervisor(s): Professor Bridgette Wessels

Professor Andrew Hoskins

Professor Martin Kretschmer

I confirm that I have read and understood the Participant Information Sheet for the above study and have had the opportunity to ask questions.

I acknowledge the provision of a Privacy Notice in relation to this research project.

I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.

I acknowledge that I will be referred to by pseudonym during the research.

I acknowledge that my personal material will be separated from research data and destroyed once the project is complete.

I acknowledge that confidentiality may not be guaranteed due to sample size.

I understand that the material will be retained in secure storage at all times including for use in future academic research.

I understand that anonymous research data will be retained for 10 years at the University of Glasgow's Enlighten.

I understand that other authenticated researchers will have access to this data only if they agree to preserve the confidentiality of the information as requested in this form.

I understand that other authenticated researchers may use my words in publications, reports, web pages, and other research outputs, only if they agree to preserve the confidentiality of the information as requested in this form

I confirm that the material may be used in future publications, both print and online.

I agree to waive my copyright to any data collected as part of this project.

I **consent / do not consent** (delete as applicable) to interviews being **audio / video** (delete as applicable) recorded on **Teams / Zoom** (delete as applicable).

I **agree / do not agree** (delete as applicable) to take part in the above study.

Name of Participant Signature

Date

Name of Researcher Signature

Date

..... End of consent form

Appendix 16: Six Themes from the Second Stage

Theme 1: Public	India	UK
Impact on Public	Awareness Political polarisation Protests	Public Awareness Normalised Abnormality Nothing is free Shaping affect Topics affected
Minority/Targeted groups	Journalists Minority NGOs	Journalism Othering-whose free speech Targeted group
Fear	Arrests Expressing opinions Secure Self-Censorship Protests	Anonymity Privacy Self-censorship
Trust	Trust	Trust Transparency Uncertainty

Theme 2: Dual-Use	India	UK
Shaping Discourse/Manipulation	Ads Algorithm Army (1) Bots Cambridge Analytica (1) Content manipulation Harmful speech Hate speech Misinformation Violent content Flagggers Shaped discourse Targeted Trolling	Advertising Algorithm Biased info Bots Cambridge Analytica (2) Fake news Manipulating Polarised Shaping discourse
Veillance	Aadhaar Data Interception Pegasus (2) Profiling/personal data Surveillance	Age verification Data Encryption Interception Pegasus (2) Phishing Profiling Surveillance
Blocks and Removals	Censorship Content Block Content control Content removal Content takedown Internet shutdown	Automated content removal Censorship Child Content takedown Harmful Illegal content Weaponised content
Tech/special cases	Army (2) Export Cambridge Analytica (2) Pegasus (2)	Export-Iran Cambridge Analytica (2) Pegasus (2)

	Techfog	

Theme 3: Rules and Regulations	India	UK
Law	Bills Broad terms Deadlock IT Rules Intermediary Liability Privacy Encryption Surveillance Traceability Santa Clara Telegraph Act	Laws (multiple) Online Safety Bill Regulation Clash Enforcement
Regulations	Anti-government Checks and Balances Free speech Indirect Pressure Over-regulation Takedown Transparency	Criticism Harmful content Legitimising impact Over regulation Regulation of tech
Individual Rights	Access to information Life and Liberty Overview Privacy Speech Problems	Individual rights Right to access
Courts	Courts	Enforcement

Theme 4: Government	India	UK
Government-National	Indian BJP Securitisation	Government Approach-Tech Elections-Free and fair Interference
Government-SMP	Facebook SMP-Gov Other SMPs Twitter	Business-Model Facebook Relationships Roles Twitter
Government-Worldwide	World	World

Theme 5: Views on SMPs	India	UK
Power and Importance	Importance Accessibility Elections Manipulation News Political importance Protests and crisis Power	Power Power-concern Power-scale Important Environment Public square Important
Goods and Bads	Good views Bad views Problematic Self-censorship Overviews	Personal uses Good use Complaints Dangerous to democracy Addiction

Theme 6: Views on Democracy	India	UK
Democracy vs Authoritarian	Authoritarian Democratic Not democratic	Authoritarian Authoritarian-China Democracy

	Should be	Democracy should Democratic Not Democratic

Appendix 17: Final Themes

	Themes and Aspects of Stage 1 and 2
Third Stage	1. -Veillance a. Operations: surveillance and dataveillance b. Role of social media platforms: government user data requests and respondents' assessment of the role of SMPs c. Legal aspect: individual rights; state laws; legal concern d. Observed implications on the public: public awareness; multi-level distrust 2. Content control: a. Operations: content blocks and removals b. Role of social media platforms: content takedowns and respondents' assessment of the role of SMPs c. Legal aspect: individual rights; state laws; legal concerns d. Observed implications on the public: public awareness and normalisation; impact on minorities; self-censorship 3. Shaped discourse a. Operations: some operations identified from FoN and interviews b. Role of social media platforms: assessments of the tools and platforms by my respondents c. Legal aspect: Individual rights; some laws; legal concerns d. Observed implications on the public: public awareness; impact on minorities; distrust

Bibliography

20C Fox v BT (2011). Available at: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/28_07_11_bt_newzbin_ruling.pdf (Accessed: 2022).

Aal, K., Krüger, M., Rohde, M., Tadic, B. and Wulf, V. (2019) 'Social Media and ICT Usage in Conflicts Areas', in Reuter, C. (ed.) *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden: Springer Fachmedien Wiesbaden, pp. 383-401.

Agrawal, A. (2021) 'Facebook, WhatsApp Sue Indian Government Over Traceability Requirement', *Forbes India*, 26 May 2021. Available at: <https://www.forbesindia.com/article/take-one-big-story-of-the-day/facebook-whatsapp-sue-indian-government-over-traceability-requirement/68175/1#:~:text=Facebook%20and%20WhatsApp%20argue%20that,Watsapp%20said%20that%20attorneys%20and> (Accessed: 2023).

Al Jazeera (2019) 'What You Need to Know About India's BJP', 23 May 2019. Available at: <https://www.aljazeera.com/news/2019/5/23/what-you-need-to-know-about-indias-bjp> (Accessed: 21 July 2023).

Allen, M. (2013) 'What was Web 2.0? Versions as the Dominant Mode of Internet History', *New Media & Society*, 15(2), pp. 260-275.

Appelrouth, S. and Edles, L. (2007) 'Readings: Anthony Giddens (1938-)', in *Sociological Theory in the Contemporary Era: Text and Readings*. Thousand Oaks, CA: Pine Forge Press, pp. 523-530.

Andrejevic, M. B. (2011) 'Surveillance and Alienation in the Online Economy', *Surveillance & Society*, 8(3), pp. 278-287.

Archer, M. S. (1982) 'Morphogenesis versus Structuration: On Combining Structure and Action', *The British Journal of Sociology*, 33(4), pp. 455-483.

Arun, T. K. (2013) 'Why the BJP is Different from the Congress', *The Times of India*, 6 August 2013. Available at: <https://timesofindia.indiatimes.com/blogs/cursor/why-the-bjp-is-different-from-the-congress/> (Accessed: 21 July 2023).

Avoid Inauthentic Sharing on Facebook (n.d.). Available at: <https://en-gb.facebook.com/business/help/2867407553519694?id=208060977200861> (Accessed: 5 July 2023).

Baseggio, E. M. d., Schneider, O. and Tresch, T. S. (2020) *Social Media and the Armed Forces*. SPRINGER.

Basuroy, T. (2023a) 'Number of Facebook Users in India from 2019 to 2028'. *Statista*. Available at: <https://www.statista.com/forecasts/1136430/facebook-users-in-india> (Accessed: 24 October 2024).

Basuroy, T. (2023b) 'Number of Internet Users in India from 2010 to 2023, With Estimates until 2050 (in millions)'. *Statista*. Available at: <https://www.statista.com/statistics/255146/number-of-internet-users-in-india/> (Accessed: 24 October 2024).

Basuroy, T. (2023c) 'Number of Twitter Users in India from 2013 to 2022'. *Statista*. Available at: <https://www.statista.com/statistics/381832/twitter-users-india/> (Accessed: 24 October 2024).

Bebawi, S. and Bossio, D. (2014) 'Introduction', in Bebawi, S. and Bossio, D. (eds.) *Social Media and the Politics of Reportage: The 'Arab Spring'*. London: Palgrave Macmillan UK, pp. 1-8.

Berg, S. and Hoffman, J. (2021) 'Digital Democracy', *Internet Policy Review*, 10(4).

Berger, P. L. and Luckmann, T. (1966) *The Social Construction of Reality: a Treatise in the Sociology of Knowledge*. New York, NY: Open Road Integrated Media.

Bhaskar, R. (1979) 'Societies', in *Philosophy and the Human Sciences: The Possibility of Naturalism : a Philosophical Critique of the Contemporary Human Sciences*. Brighton: Harvester Press, pp. 31-69.

Bijker, W. E. and Pinch, T. J. (2012) 'The Social Construction of Facts and Artifacts: Or how the Sociology of Science and the Sociology of Technology Might Benefit Each Other', in Bijker, W. E., Hughes, T. P. and Pinch, T. J. (eds.) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Anniversary edn. London; Cambridge, MA: MIT Press, pp. 11-45.

Boje, T. P. (2021) 'Introduction to Civility and Participatory Democracy', in Boje, T. P. (ed.) *Civility and Participatory Democracy: the Importance of Civil Society and Active Citizenship*. Northampton: Edward Elgar Publishing, pp. 1-7.

Bowen, G. A. (2009) 'Document Analysis as a Qualitative Research Method', *Qualitative Research Journal*, 9(2), pp. 27-40.

- Boyd, d. (2010) 'Social Network Sites as Networked Publics' in Papacharissi, Z. (Ed.), *A Networked Self : Identity, Community, and Culture on Social Network Sites*. Oxford, United Kingdom: Taylor and Francis Group, pp. 46-68.
- Bradshaw, S., Campbell-Smith, U., Henle, A., Prini, A., Shalev, S., Bailey, H. and Howard, P. N. (2021) *Country Case Studies: Industrialized Disinformation: 2020, Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute. Available at: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/03/Case-Studies_FINAL.pdf (Accessed: 26 June 2023).
- Brancati, D. (2014) 'Democratic Authoritarianism: Origins and Effects', in Levi, M. and Rosenblum, N. (eds.) *Annual Review of Political Science*. Palo Alto: Annual Reviews, pp. 313-326.
- Brandt, J. (2022) *Digital Authoritarianism: Patways, Trends, Solutions*. Available at: https://www.concordia.ca/content/dam/artsci/research/migs/docs/MIGS_Report_Digital_Authoritarianism_2022.pdf (Accessed: 30 August 2022).
- Braun, V. and Clarke, V. (2013) *Successful Qualitative Research: a Practical Guide for Beginners*. London: SAGE.
- Brown, C. (2019) *Understanding International Relations*. London: Bloomsbury Publishing Plc.
- Brown, T. (2022) Digital Economy Act 2017 (Commencement of Part 3) Bill [HL]. Available at: <https://lordslibrary.parliament.uk/digital-economy-act-2017-commencement-of-part-3-bill-hl/> (Accessed: 2023).
- Brownlee, J. (2007) *Authoritarianism in an Age of Democratization*. Cambridge: Cambridge University Press.
- Buchanan, E. A. and Zimmer, M. (2012) 'Internet Research Ethics', in Zalta, E. (ed.) *The Stanford Encyclopedia of Philosophy*. Available at: <https://plato.stanford.edu/entries/ethics-Internet-research/> (Accessed: 16 March 2024).
- Bulk Acquisition of Communications Data: Code of Practice (2018). Available at: https://assets.publishing.service.gov.uk/media/6401e251e90e0740dafbbbf/Bulk_Communications_Data_Code_of_Practice.pdf (Accessed: 2022).

Bulovsky, A. (2019) 'Authoritarian Communication on Social Media: The Relationship Between Democracy and Leaders' Digital Communicative Practices', *The International Communication Gazette*, 81(1), pp. 20-45.

Burgess, J., Marwick, A. and Poell, T. (2018) 'The SAGE Handbook of Social Media', in SAGE Publications Ltd. Available at: <https://sk.sagepub.com/reference/the-sage-handbook-of-social-media> (Accessed: 2 April 2024).

Buzan, B., Wæver, O. and Wilde, J. D. (1997) *Security : A New Framework for Analysis*. Boulder, CO, United States: Lynne Rienner Publishers.

Cadwalladr, C. and Graham-Harrison, E. (2018) 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach', *The Guardian*, 17 March 2018. Available at: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (Accessed: 2020).

Cameron, D. (2001) *Working with spoken discourse*. London: SAGE.

Carlo, S., Hurfurt, J. and Johnson, M. (2023) *Ministry of Truth: The Secretive Government Units Spying on Your Speech*. Big Brother Watch. Available at: <https://bigbrotherwatch.org.uk/wp-content/uploads/2023/01/Ministry-of-Truth-Big-Brother-Watch-290123.pdf> (Accessed: 11 July 2023).

Carr, C. T. and Hayes, R. A. (2015) 'Social Media: Defining, Developing, and Divining', *Atlantic Journal of Communication*, 23(1), pp. 46-65.

Centre for Data Ethics and Innovation (2022) *Public Attitudes to Data and AI: Tracker Survey*. London: CDEI. Available at: https://assets.publishing.service.gov.uk/media/62d6a7998fa8f50c0068506f/Public_Attitudes_to_Data_and_AI_-_Tracker_Survey.pdf (Accessed: 10 November 2025).

Centre for Data Ethics and Innovation (2019) *Snapshot Paper - Deepfakes and Audiovisual Disinformation*. London: CDEI. Available at: <https://www.gov.uk/government/publications/cdei-publishes-its-first-series-of-three-snapshot-papers-ethical-issues-in-ai/snapshot-paper-deepfakes-and-audiovisual-disinformation#about-the-cdei> (Accessed: 19 October 2022).

Chadwick, A. (2006) *Internet Politics: States, Citizens, and New Communication Technologies*. New York: Oxford University Press, Inc.

Chang, C.-C. and Lin, T.-H. (2020) 'Autocracy Login: Internet Censorship and Civil Society in the Digital Age', *Democratization*, 27(5), pp. 874-895.

Chang, E. and Golden, M. A. (2010) 'Sources of Corruption in Authoritarian Regimes', *Social Science Quarterly*, 91(1), pp. 1-20.

Clark, D. (2024) 'Population of the United Kingdom from 1937 to 2023, by Gender'. 7 December 2024. Office for National Statistics (UK). Available at: <https://www.statista.com/statistics/281240/population-of-the-united-kingdom-uk-by-gender/> (Accessed: 2024).

Clarke, V. and Braun, V. (2017) 'Thematic Analysis', *The Journal of Positive Psychology*, 12(3), pp. 297-298.

Clift, S. (1998) 'Democracy is Online', *On the Internet Magazine*. Available at: <https://www.publicus.net/articles/democracyonline.html> (Accessed: 2022).

Clinton, H. R. (2010) *Remarks on Internet Freedom*. Available at: <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm> (Accessed: 24 October 2023).

Colebatch, H. K. (2014) 'Making Sense of Governance', *Policy & Society*, 33(4), pp. 307-316.

Collins, A. and Morgan, P. (2022) *Contemporary Security Studies*. Oxford University Press.

The Constitution (Forty-Second amendment) Act (1976). Available at: <https://legislative.gov.in/constitution-forty-second-amendment-act-1976> (Accessed: 2022).

The Constitution of India (1950). Available at: <https://legislative.gov.in/sites/default/files/Savidhan.pdf> (Accessed: 2022).

The Constitution of India (Sixteenth Amendment) Act (1963). Available at: <https://www.india.gov.in/my-government/constitution-india/amendments/constitution-india-sixteenth-amendment-act-1963&ved=2ahUKEwiXhKSI7MaRAXwQ0EAHV0lBj0QFnoECC0QAQ&usg=AOvVaw1XZPrLLMBTCjwag44FktV-> (Accessed: 2025).

The Copyright Act (1957). Available at: <https://www.copyright.gov.in/Documents/Copyrightrules1957.pdf> (Accessed: 2022).

The Copyright (Amendment) Act (2012). Available at: https://copyright.gov.in/Documents/Notification/Copyright_Amendment_2012.pdf (Accessed: 12 October 2025).

Copyright, Designs and Patents Act (1988). Available at: <https://www.legislation.gov.uk/ukpga/1988/48/contents> (Accessed: 2023).

Cormode, G. and Krishnamurthy, B. (2008) 'Key Differences Between Web 1.0 and Web 2.0', *First Monday*, 13 (6).

CSDS-Lokniti (2019) *Social Media & Public Behaviour*. New Delhi: Centre for Study of Developing Societies. Available at: https://www.lokniti.org/media/upload_files/Social%20media%20and%20Political%20Behaviour%20report%20new.pdf (Available at: 20 October 2025).

CSDS-Lokniti (2023) *Status of Policing in India Report 2023: Surveillance and the Question of Privacy*. New Delhi: Centre for Study of Developing Societies. Available at: https://drive.google.com/file/d/1e7sZfuBrwi0suNTN5UBncFubxTJE_Ga6/view (Accessed: 20 October 2025).

Dahl, R. A. (1989) *Democracy and Its Critics*. London; New Haven: Yale University Press.

Dahl, R. A. (2000) *On Democracy*. New Haven, Conn; London: Yale University Press.

Dalek, J., Marczak, B., McKune, S., Noor, N., Oliver, J., Penney, J., Senft, A. and Deibert, R. (2018) *Planet Netsweeper: Section 2 - Country Case Studies*. Toronto: Citizen Lab. Available at: <https://citizenlab.ca/2018/04/planet-netsweeper-section-2-country-case-studies/> (Accessed: 05 August 2022).

Data Protection Act (2018). Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 26 May 2023).

Department of Digital, Culture, Media, and Sport (2019) *Disinformation and 'Fake News': Final Report* (HC 1791). Available at: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf> (Accessed: 19 October 2022).

De Vaus, D. A. (2001) *Research Design in Social Research*. London: Sage.

Deibert, R. (2015) 'Authoritarianism Goes Global: Cyberspace Under Siege', *Journal of Democracy*, 26(3), pp. 64-78.

Deibert, R. and Crete-Nishihata, M. (2012) 'Global Governance and the Spread of Cyberspace Controls', *Global Governance*, 18(3), pp. 339-361.

Denzin, N. K. (1989) *The Research Act in Sociology: a Theoretical Introduction to Sociological Methods*. 3rd edn. London: Butterworths.

Devlin, K. (2019) *A Sampling of Public Opinion in India*. Available at: <https://www.pewresearch.org/global/2019/03/25/a-sampling-of-public-opinion-in-india/> (Accessed: 16 October 2025).

Devolution: Factsheet (n.d.). Available at: <https://assets.publishing.service.gov.uk/media/5c38cc6ce5274a70ca3c3cef/DevolutionFactsheet.pdf> (Accessed: 25 January 2024).

Diamond, L. (2002) 'Thinking About Hybrid Regimes', *Journal of Democracy*, 13(2), pp. 21-35.

Diamond, L. (2010) 'Liberation Technology', *Journal of Democracy*, 21(3), pp. 69-83.

Digital Economy Act (2017). Available at: <https://www.legislation.gov.uk/ukpga/2017/30/contents> (Accessed: 2022).

The Digital Personal Data Protection Act (2023). Available at: <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf> (Accessed: 2024).

The Disaster Management Act (2005). Available at: https://ndma.gov.in/sites/default/files/PDF/DM_act2005.pdf (Accessed: 2023).

Dunne, T. (2023) ' Liberal Internationalism', in Baylis, J., Smith, S. and Owens, P. (eds.) *The Globalization of World Politics: An Introduction to International Relations*. Oxford University Press.

The Economic Times (2021) 'Govt asks people to register as cyber crime volunteers to check unlawful online content', *The Economic Times*, 09 February 2021. Available at: <https://economictimes.indiatimes.com/tech/technology/govt-asks-people-to-register-as-cyber-crime-volunteers-to-check-unlawful-online-content/articleshow/80768314.cms> (Accessed: 2022).

Edelman (2022) *Trust in Technology- APAC Report*. Available at: https://www.edelman.in/sites/g/files/aatuss371/files/2022-10/2022%20Edelman%20Trust%20Barometer%20Special%20Report_Trust%20in%20Technology_APAC%20Region%20Report.pdf (Accessed: 20 October 2025).

Edwards, A., Webb, H., Housley, W., Beneito-Montagut, R., Procter, R. and Jirotko, M. (2021) 'Forecasting the Governance of Harmful Social Media Communications: Findings from the Digital Wildfire Policy Delphi', *Policing & Society*, 31(1), pp. 1-19.

The Electoral Commission (2023) *Public Opinion Tracker*. Available at: <https://www.electoralcommission.org.uk/research-reports-and-data/public-attitudes/public-attitudes-2023> (Accessed: 20 October 2025).

Erixon, F. and Lee-Makiyama, H. (2011) *Digital Authoritarianism: Human Rights, Geopolitics and Commerce*. Brussels: ECIPE. Available at: <https://ecipe.org/wp-content/uploads/2014/12/digital-authoritarianism-human-rights-geopolitics-and-commerce.pdf> (Accessed: 2020).

Etlinger, S. (2019) *What's So Difficult About Social Media Platform Governance?* Centre for International Governance. Available at: <http://www.jstor.org/stable/resrep26127.6> (Accessed: 23 March 2024).

Evans, E. (2020) 'Gender and Political Representation', in Garnett, M. (ed.) *The Routledge Handbook of British Politics and Society*, pp. 177-187.

Export Control Joint Unit (2021) *Export Controls: Dual-use Items, Software and Technology, Goods for Torture and Radioactive Sources*. Available at: <https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources> (Accessed: 2021).

Express News Service (2022) 'Amnesty India Chair Aakar Patel Stopped at Bengaluru Airport from Travelling to US', *The Indian Express*, 7 April 2022. Available at: <https://indianexpress.com/article/cities/bangalore/aakar-patel-stopped-at-bengaluru-airport-amnesty-india-cbi-case-7854994/> (Accessed: 8 April 2023).

Eynon, R., Fry, J. and Schroeder, R. (2017) 'The SAGE Handbook of Online Research Methods', in SAGE Publications Ltd. Available at: <https://sk.sagepub.com/reference/the-sage-handbook-of-online-research-methods-2e>.

Feenberg, A. (2017) *Technosystem : The Social Life of Reason*. Cambridge, United States: Harvard University Press.

Fielding, N. and Thomas, H. (2015) 'Qualitative Interviewing', in Gilbert, G. N. (ed.) *Researching Social Life*. 4th edn. London: SAGE Publications, pp. 281-300.

Flyverbom, M., Deibert, R. and Matten, D. (2019) 'The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business', *Business & Society*, 58(1), pp. 3-19.

Ford, M. C. and Hoskins, A. (2022) *Radical War: Data, Attention and Control in the Twenty-First Century*. New York, NY: Oxford University Press.

Freedom of Information Act (2000). Available at: <https://www.legislation.gov.uk/ukpga/2000/36/introduction> (Accessed: 2023).

Freedom of Information (Scotland) Act (2002). Available at: <https://www.legislation.gov.uk/asp/2002/13/contents> (Accessed: 2023).

Freedom House (n.d.) *Our History*. Available at: <https://freedomhouse.org/about-us/our-history> (Accessed: 2021).

Freedom on the Net- About Freedom on the Net (n.d.). Available at: <https://freedomhouse.org/report/freedom-net> (Accessed: 2021).

Fuchs, C. (2024) *Social media: a critical introduction*. 4th edn.). Thousand Oaks: SAGE Publications Ltd.

Fukuyama, F. (1989) 'The End of History?', *The National Interest*, (16), pp. 3-18.

Fukuyama, F. (2013) 'What Is Governance?', *Governance*, 26(3), pp. 347-368.

Gadodia, M., Mukherji, S. and Kulkarni, T. (2023) *History and Development of John Doe Orders in India*. Available at: <https://www.livelaw.in/law-firms/law-firm-articles-/john-doe-order-fifa-world-cup-quia-timet-civil-procedure-code-delhi-high-court-non-fungible-token-220689#:~:text=A%20John%20Doe%20order%20is%20a%20type%20of%20legal%20order,legal%20action%20is%20being%20taken> (Accessed: 2024).

Garnett, M., Dorey, P. and Lynch, P. (2021) *Exploring British Politics*. 5th edn. Abingdon, Oxon: Routledge.

Gearhart, S. and Zhang, W. (2015) "'Was it something I said?' 'No, it was something you posted!' A study of the spiral of silence theory in social media contexts'. *Cyberpsychology, Behavior and Social Networking*, 18(4), pp. 208-213.

Gee, J. P. (2014) *An introduction to discourse analysis: theory and method* (Fourth ed.). Abingdon, Oxon: Routledge.

George, A. L. and Bennett, A. (2004) *Case Studies and Theory Development in the Social Sciences*. London; Cambridge, Mass: MIT Press.

Gibson, J. J. (2015) *The ecological approach to visual perception*. Classic edn. New York; Hove, England: Psychology Press.

Giddens, A. (1984) *The Constitution of Society: Outline of the Theory of Structuration*. Malden, Mass; Cambridge, England: Polity Press.

Gilbert, L. and Mohseni, P. (2011) 'Beyond Authoritarianism: The Conceptualization of Hybrid Regimes', *Studies in Comparative International Development*, 46(3), pp. 270-297.

Gill, P. (2020) 'India's Three Main Surveillance Projects NATGRID, CMS and NETRA Have Been Directed to Stop Collecting Data Citing Breach of Privacy', *Business Insider India*. Available at: <https://www.businessinsider.in/tech/news/indias-three-main-surveillance-projects-natgrid-cms-and-netra-have-been-directed-to-stop-collecting-data-citing-breach-of-privacy/articleshow/79529256.cms> (Accessed: 8 May 2023).

Gleicher, N. (2019) *Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan*. Available at: <https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/> (Accessed: 2023).

Global Data (n.d.) 'Female Population in India (2010 - 2021)'. Available at: <https://www.globaldata.com/data-insights/macroeconomic/female-population-in-india-2095923/> (Accessed: 2023).

Gorwa, R. and Ash, T. G. (2020) 'Democratic Transparency in the Platform Society', in Persily, N. and Tucker, J. A. (eds.) *Social Media and Democracy*. Cambridge: Cambridge University Press, pp. 286-312.

GOV.UK (2014) *Covert Surveillance Code of Practice*. Available at: <https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice> (Accessed: 2024).

GOV.UK (2020) *NHS Test and Trace: What to Do if You are Contacted*. Available at: <https://www.gov.uk/guidance/nhs-test-and-trace-how-it-works#:~:text=If%20NHS%20Test%20and%20Trace%20contacts%20you%2C%20the%20service%20will,phone%20number%200300%20013%205000> (Accessed: 28 April 2024).

Gray, D. (2018) *Doing Research in the Real World*. 4th edn. London: SAGE Publications Ltd.

Gray, L., Wong Wylie, G., Rempel, G. and Cook, K. (2020) 'Expanding Qualitative Research Interviewing Strategies: Zoom Video Communications', *The Qualitative Report*, 25(Number 5, Article 8), pp. 1292-1301.

Gregory, J. (2022) 'Three PMs in Two Months, is Political Chaos the UK's New Normal?', *BBC*, 26 October 2022. Available at: <https://www.bbc.co.uk/news/uk-63383616> (Accessed: 26 January 2024).

Groups Within 77th Brigade (n.d.). Available at: <https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/groups/> (Accessed: 11 July 2023).

Gunitsky, S. (2015) 'Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability', *Perspectives on Politics*, 13(1), pp. 42-54.

Hague, B. N. and Loader, B. (1999) *Digital Democracy: Discourse and Decision Making in the Information Age*. London; New York: Routledge.

Hakeem, M. J. and Sulphrey, M. M. (2023) 'The Role of Civil Society in India and Afghanistan: A Comparative Perspective', *Journal of Asian and African Studies*, 60(2), pp. 926-946.

Hakim, C. (2000) 'Research Reviews, Meta-analysis and Secondary Analysis', in *Research Design: Successful Designs for Social and Economic Research*. 2nd edn. London: Routledge, pp. 21-33.

Held, D. (2006) *Models of Democracy*. 3rd edn. Cambridge: Polity Press.

Hesse-Biber, S. N., Rodriguez, D. and Frost, N. A. (2015) 'Qualitatively Driven Approach to Multimethod and Mixed Methods Research', in Hesse-Biber, S. N. and Johnson, R. B. (eds.) *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*. Oxford: Oxford University Press, pp. 3-20.

Hill, K. (2022) 'A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.', *The New York Times*, 22 August 2022. Available at:

<https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html> (Accessed: 2023).

Hobson, C. (2015) *The Rise of Democracy: Revolution, War and Transformations in International Politics Since 1776*. Edinburgh: Edinburgh University Press.

Home Office (2018) *New Technology Revealed to Help Fight Terrorist Content Online*. Available at: <https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online> (Accessed: 2022).

House of Commons Library (2023) *The Data Protection and Digital Information Bill 2022-23*. Available at: <https://commonslibrary.parliament.uk/research-briefings/cbp-9606/> (Accessed: 24 September 2024).

Howells, L. and Henry, L. A. (2021) 'Varieties of Digital Authoritarianism', *Communist and Post-Communist Studies*, 54(4), pp. 1-27.

Hughes, T. P. (2012) 'The Evolution of Large Technological Systems', in Bijker, W. E., Hughes, T. P. and Pinch, T. J. (eds.) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Anniversary edn. London; Cambridge, MA: MIT Press, pp. 45-77.

Human Rights Act, Schedule I- The Articles (1998). Available at: <https://www.legislation.gov.uk/ukpga/1998/42/schedule/1> (Accessed: 2022).

Hunter, A. and Brewer, J. D. (2015) 'Designing Multimethod Research', in Hesse-Biber, S. N. and Johnson, R. B. (eds.) *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*. Oxford: Oxford University Press, pp. 185-205.

Huntington, S. P. (1991) 'Democracy's Third Wave', *Journal of Democracy*, 2(2), pp. 12-34.

Hutchby, I. (2001) 'Technologies, Texts and Affordances', *Sociology*, 35(2), pp. 441-456.

International Federation of Journalists (2021) *India: Journalists Targeted for Reporting Farmer Protest*. Available at: <https://www.ifj.org/media-centre/news/detail/article/india-journalists-targeted-for-reporting-farmer-protest> (Accessed: 2023).

India-Facebook (n.d.-a) *Content Restrictions Based on Local Law*. Available at: <https://transparency.fb.com/data/content-restrictions/country/IN/> (Accessed: 2 April 2022).

India-Facebook (n.d.-b) *Government Requests for User Data - India*. Available at: <https://transparency.fb.com/data/government-data-requests/country/IN/> (Accessed: 2 April 2022).

India-FiW (2020) *India - Freedom in the World 2020*. Freedom House. Available at: <https://freedomhouse.org/country/india/freedom-world/2020> (Accessed: 2021).

India-FiW (2021) *India - Freedom in the World 2021*. Freedom House. Available at: <https://freedomhouse.org/country/india/freedom-world/2021> (Accessed: 2021).

India-FiW (2022) *India - Freedom in the World 2022*. Freedom House. Available at: <https://freedomhouse.org/country/india/freedom-world/2022> (Accessed: 2022).

India-FoN (2019) *India - Freedom on the Net 2019*. Freedom House. Available at: <https://freedomhouse.org/country/india/freedom-net/2019> (Accessed: 2021).

India-FoN (2020) *India - Freedom on the Net 2020*. Freedom House. Available at: <https://freedomhouse.org/country/india/freedom-net/2020> (Accessed: 2021).

India-FoN (2021) *India - Freedom on the Net 2021*. Freedom House. Available at: <https://freedomhouse.org/country/india/freedom-net/2021> (Accessed: 2021).

India-Twitter (n.d.-a) *Government Information Request*. Available at: <https://transparency.twitter.com/en/reports/countries/in.html> (Accessed: 2 April 2022).

India-Twitter (n.d.-b) *Government Removal Request*. Available at: <https://transparency.twitter.com/en/reports/countries/in.html> (Accessed: 2 April 2022).

India-Twitter-Web Archive (2022) *India-Twitter Transparency Center*. Available at: <https://web.archive.org/web/20220303184651/https://transparency.twitter.com/en/reports/countries/in.html> (Accessed: 9 November 2024).

The Indian Penal Code (1860). Available at: <https://www.indiacode.nic.in/repealedfileopen?rfilename=A1860-45.pdf> (Accessed: 12 October 2025).

Indian Telegraph Act (1885). Available at:
https://dot.gov.in/sites/default/files/the_indian_telegraph_act_1985_pdf.pdf
 (Accessed: 2022).

The Indian Telegraph Rules (1951). Available at:
<https://thc.nic.in/Central%20Governmental%20Rules/Indian%20Telegraph%20Rules,1951.pdf?ref=static.internetfreedom.in> (Accessed: 12 October 2025).

Information and Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules (2009). Available at:
<https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28%20Procedure%20and%20safeguards%20for%20blocking%20for%20access%20of%20information%20by%20public%29%20Rules%2C%202009.pdf> (Accessed: 2022).

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021). Available at:
https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf (Accessed: 19 August 2022).

Information Technology Act (2000). Available at:
<https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijm uixngudufgbuubgubfugbububjxcgfvdbihbgfGhdfgFHytyhRtMjk4NzY=> (Accessed: 2022).

The Information Technology Act (2008). Available at:
[https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20\(amendment\).pdf](https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf) (Accessed: 2022).

Investigatory Powers Act (2016). Available at:
<https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted> (Accessed: 2022).

Investigatory Powers Tribunal (n.d.) *Welcome to the Investigatory Powers Tribunal website*. Available at:
<https://investigatorypowertribunal.org.uk/#:~:text=The%20Investigatory%20Powers%20Tribunal%20is,authority%20using%20covert%20investigative%20techniques>
 (Accessed: 2023).

Internet Watch Foundation (n.d.) *Who we are*. Available at:
<https://www.iwf.org.uk/about-us/who-we-are/> (Accessed: 6 April 2023).

Jain, B. (2019) 'Lok Sabha Elections: At 67.1%, 2019 Turnout's a Record, Election Commission Says', *Times of India*, 21 May 2019. Available at:

<https://timesofindia.indiatimes.com/india/at-67-1-2019-turnouts-a-record-election-commission/articleshow/69419715.cms?from=mdr> (Accessed: 19 January 2024).

Jha, M. K. and Choubey, K. N. (2023) *Indian Politics and Political Processes: Ideas, Institutions and Practices*. Place of publication not identified: Routledge.

Jiang, M. (2010) 'Authoritarian Informationalism: China's Approach to Internet Sovereignty', *The SAIS Review of International Affairs*, 30(2), pp. 71-89.

Justice Initiative (2012) *Margin of Appreciation*. Available at: <https://www.justiceinitiative.org/uploads/918a3997-3d40-4936-884b-bf8562b9512b/echr-reform-margin-of-appreciation.pdf> (Accessed: 2023).

Kaplan, A. M. and Haenlein, M. (2010) 'Users of the World, Unite! The Challenges and Opportunities of Social Media', *Business Horizons*, 53(1), pp. 59-68.

Katakam, A. (2021) 'Bhima Koregaon Case: Planted Evidence?', *The Hindu*, 27 February 2021. Available at: <https://frontline.thehindu.com/the-nation/bhima-koregaon-case-planted-evidence-in-rona-wilson-computer-according-to-arsenal-consulting-investigation/article33887640.ece> (Accessed: 24 May 2023).

Kawerau, L., Weidmann, N. B. and Dainotti, A. (2023) 'Attack or Block? Repertoires of Digital Censorship in Autocracies', *Journal of Information Technology & Politics*, 20(1), pp. 60-73.

Kemp, S. (2019) *Digital 2019: Global Digital Overview*. Available at: <https://datareportal.com/reports/digital-2019-global-digital-overview>.

Khan, T. H. and MacEachen, E. (2022) 'An Alternative Method of Interviewing: Critical Reflections on Videoconference Interviews for Qualitative Data Collection', *International Journal of Qualitative Methods*, 21, pp. 1-12.

Klein, H. K. and Kleinman, D. L. (2002) 'The Social Construction of Technology: Structural Considerations', *Science, Technology, & Human Values*, 27(1), pp. 28-52.

Komaitis, K. and Carter, J. (2023) *Internet Governance and Digital Governance: Are They the Same Thing?* Available at: <https://techpolicy.press/internet-governance-and-digital-governance-are-they-the-same-thing/> (Accessed: 30 October 2023).

- Kramer, S. (2021) *Religious Composition of India*. Available at: <https://www.pewresearch.org/religion/2021/09/21/religious-composition-of-india/> (Accessed: 18 August 2022).
- Kreiss, D. and McGregor, S. C. (2017) 'Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S Presidential Cycle', *Political communication*, 35(2), pp. 155-177.
- Krekó, P. (2021) 'How Authoritarians Inflate Their Image', *Journal of Democracy*, 32(3), pp. 109-123.
- Levitsky, S. and Way, L. A. (2002) 'The Rise of Competitive Authoritarianism', *Journal of Democracy*, 13(2), pp. 51-65.
- Liang, F., Das, V., Kostyuk, N. and Hussain, M. M. (2018) 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure', *Policy and Internet*, 10(4), pp. 415-453.
- Lindgren, S. (2022) 'Social Media Platforms', in *Digital Media and Society*. 2nd edn. Thousand Oaks: SAGE Publications Ltd. Chapter 2.
- Linz, J. (2000) *Totalitarian and Authoritarian Regimes*. London; Boulder, CO: Lynne Rienner Publishers.
- Lipschultz, J. H. (2022) *Social Media and Political Communication*. New York: Routledge.
- Liu, J. (2020) 'China's Data Localization', *Chinese Journal of Communication*, 13(1), pp. 84-103.
- MacAskill, E. (2014) 'Putin Calls Internet a 'CIA project' Renewing Fears of Web Breakup', *The Guardian*, 24 April 2014. Available at: <https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia> (Accessed: 13 October 2023).
- MacAskill, E., Borger, J., Hopkins, N., Davies, N. and Ball, J. (2013) 'GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications', *The Guardian*, 21 June. Available at: <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> (Accessed: 29 March 2021).
- MacAskill, E. and Dance, G. (2013) *NSA Files: Decoded*. Available at: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> (Accessed: 29 March 2021).

MacKinnon, R. (2011) 'China's 'Networked Authoritarianism'', *Journal of Democracy*, 22(2), pp. 32-46.

MacKinnon, R. (2012) *Contested of the Networked*. Kindle. Basic Books: Perseus Books Group.

Mance, H., Fildes, N. and Hughes, L. (2018) 'Conservatives Criticised for Links to Cambridge Analytica', *Financial Times*, 21 March 2018. Available at: <https://www.ft.com/content/29a2d524-2d32-11e8-a34a-7e7563b0b0f4> (Accessed: 11 December 2023).

Mann, S. (2013) 'Veilance and reciprocal transparency: Surveillance versus sousveillance, AR glass, lifelogging, and wearable computing', *2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmented Reality in Everyday Life*. Toronto, ON, Canada. Pp. 1-12.

Mason, J. (2006) 'Mixing Methods in a Qualitatively Driven Way', *Qualitative Research : QR*, 6(1), pp. 9-25.

Mason, M. (2010) 'Sample Size and Saturation in PhD studies Using Qualitative Interviews', *Forum, Qualitative Social Research*, 11(3), pp. 1-19.

Medeiros, B. P. and Goldoni, L. R. F. (2020) 'The Fundamental Conceptual Trinity of Cyberspace', *Contexto internacional*, 42(1), pp. 31-54.

Menlo Security (2023) *Level of trust among consumers that selected digital advertising platforms did not serve malvertising in the United Kingdom as of June 2023*. Available at: <https://www.statista.com/statistics/1394360/trust-digital-advertising-malvertising-uk/> (Accessed: 26 October 2025).

Merkel, W. (2004) 'Embedded and Defective Democracies', *Democratization*, 11(5), pp. 33-58.

META (n.d.) *Content Restrictions Based on Local Law*. Available at: <https://transparency.meta.com/reports/content-restrictions/> (Accessed: 30 April 2024).

Meta Ad Library Report: India (n.d.). Available at: <https://www.facebook.com/ads/library/report/?source=onboarding> (Accessed: 8 November 2024).

Meta Ad Library Report: United Kingdom (n.d.). Available at: <https://www.facebook.com/ads/library/report/?source=onboarding> (Accessed: 8 November 2024).

Michaelsen, M. (2017) 'Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran', *Surveillance & Society*, 15(3-4), pp. 465-470.

Michaelsen, M. (2018a) 'Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State', *Globalizations*, 15(2), pp. 248-264.

Michaelsen, M. (2018b) 'Transforming Threats to Power: The International Politics of Authoritarian Internet Control in Iran', *International Journal of Communication*, 12, pp. 3856-3876.

Miller, S. (2018) *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Cham: Springer International Publishing.

Milmo, C. (2010) 'Stonewall is Split by Row About Same-sex Marriages', *The Independent*, 2 October 2010. Available at: <https://www.independent.co.uk/news/uk/home-news/stonewall-is-split-by-row-about-samesex-marriages-2095468.html> (Accessed: 5 December 2024).

Mohdin, A., Swann, G. and Bannock, C. (2020) 'How George Floyd's Death Sparked a Wave of UK Anti-racism Protests', *The Guardian*, 29 July 2020. Available at: <https://www.theguardian.com/uk-news/2020/jul/29/george-floyd-death-fuelled-anti-racism-protests-britain> (Accessed: 29 February 2024).

Mollah, A. H. (2019) 'Governance', in Romaniuk, S., Thapa, M. and Marton, P. (eds.) *The Palgrave Encyclopedia of Global Security Studies*. Cham: Springer International Publishing, pp. 1-6.

Moore, N. (2007) '(Re)Using Qualitative Data?', *Sociological Research Online*, 12(3), pp. 1-13.

Morgus, R. (2019) *The Spread of Russia's Digital Authoritarianism*. Available at: <https://www.jstor.org/stable/pdf/resrep19585.17.pdf> (Accessed: 13 October 2023).

Newsroom Staff (2022) 'INDIA Fact-checker Zubair Arrested for 'Promoting Enmity', Twitter Erupts', *Newsroom Post*, 27 June 2022. Available at: <https://newsroompost.com/india/fact-checker-zubair-arrested-for-promoting-enmity-twitter-erupts/5127163.html> (Accessed: 8 April 2023).

Noelle-Neumann, E. (1974) 'The Spiral of Silence A Theory of Public Opinion'. *Journal of communication*, 24(2), pp. 43-51.

O'Connor, H. and Madge, C. (2017) 'The SAGE Handbook of Online Research Methods', in SAGE Publications Ltd. Available at: <https://sk.sagepub.com/reference/the-sage-handbook-of-online-research-methods-2e> (Accessed: 2024).

O'Loughlin, B. (2020) 'Media Regime Disruption and the Conditions of Public Reflexivity', *International Journal of Communication*, 14, pp. 6113-6132.

O'Neil, A. (2023) 'India- Statistics & Facts'. 19 January 2024. *Statista*: IMF. Available at: <https://www.statista.com/statistics/263766/total-population-of-india/> (Accessed: 2024).

O'Reilly, T. (2007) 'What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software', *Communications & Strategies*, No. 1, pp. 17-37.

Obama, B. (2013) *Statement by the President*. Available at: <https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president> (Accessed: 2022).

Ofcom (2023) *Adults' Media Use and Attitudes Report 2023*. Available at: <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes-2023/adults-media-use-and-attitudes-report-2023.pdf?v=329409> (Accessed: 24 October 2025).

The Office for the United Nations High Commissioner for Human Rights (2019) *Resolution Adopted by the Human Rights Council on 26 September 2019*. Available at: <https://docs.un.org/en/A/HRC/RES/42/15> (Accessed: 2023).

Oltmann, S. (2015) 'Dual Use Research: Investigation Across Multiple Science Disciplines', *Science and Engineering Ethics*, 21(2), pp. 327-341.

Online Harms White Paper (2020). Available at: <https://www.gov.uk/government/consultations/online-harms-white-paper> (Accessed: 6 April 2023).

Online Safety Act (2023). Available at: <https://www.legislation.gov.uk/ukpga/2023/50/enacted> (Accessed: 2024).

Office for National Statistics (2024) 'Trust in government, UK: 2023'. Available at:

<https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/bulletins/rustingovernmentuk/2023> (Accessed: 22 October 2025).

Orlikowski, W. J. (1992) 'The Duality of Technology: Rethinking the Concept of Technology in Organizations', *Organization science* (Providence, R.I.), 3(3), pp. 398-427.

Osborne, T. (2023) 'Inside the Dystopian 'HateLab' That's Surveilling Social Media', *Spiked*. Available at: <https://www.spiked-online.com/2023/12/11/inside-the-dystopian-hatelab-thats-surveilling-social-media/> (Accessed: 2024).

Owen, J. M. (2018) 'Liberal Approaches', in Gheciu, A. and Wohlforth, W. C. (eds.) *The Oxford Handbook of International Security*. Oxford University Press, pp. 100-115.

Park, N. (2020) *Population Estimates for the UK, England and Wales, Scotland and Northern Ireland: mid-2019*. Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/bulletins/annualmidyearpopulationestimates/mid2019estimates> (Accessed: 5 December 2024).

Paul, K. and Milmo, D. (2021) 'Facebook Putting Profit Before Public Good, Says Whistleblower Frances Haugen', *The Guardian*, 4 October 2021. Available at: <https://www.theguardian.com/technology/2021/oct/03/former-facebook-employee-frances-haugen-identifies-herself-as-whistleblower> (Accessed: 24 October 2023).

Peace, T. and Meer, N. (2020) 'Ethnic Diversity', in Garnett, M. (ed.) *The Routledge Handbook of British Politics and Society*. pp. 188-198.

Piccone, T. (2017) *Democracy and Cybersecurity*. Available at: https://www.brookings.edu/wp-content/uploads/2017/08/fp_20170905_democracy_cyber_security.pdf (Accessed: 24 October 2023).

Poell, T., Nieborg, D. and van Dijck, J. (2019) 'Platformisation', *Internet Policy Review*, 8(4), pp. 1-13.

Polyakova, A. and Meserole, C. (2019) *Exporting Digital Authoritarianism: The Russian and Chinese Models*. Available at: <https://www.brookings.edu/research/exporting-digital-authoritarianism/> (Accessed: 15 May 2022).

Poonam, S. and Bansal, S. (2019) 'Misinformation is Endangering India's Election', *The Atlantic*, 1 April 2019. Available at: <https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/> (Accessed: 27 June 2023).

Porter, T. and Tan, N. (2023) 'Introduction: Democracy and Digitization', *Globalizations*, 20(1), pp. 132-136.

Privacy International (2020a) *The Use of Social Media Monitoring by Local Authorities - Who is a Target?* Available at: <https://privacyinternational.org/explainer/3587/use-social-media-monitoring-local-authorities-who-target> (Accessed: 23 May 2023).

Privacy International (2020b) *When Local Authorities Aren't Your Friends*. Available at: <https://privacyinternational.org/report/3584/when-local-authorities-arent-your-friends> (Accessed: 23 May 2023).

Pye, L. W. (1990) 'Political Science and the Crisis of Authoritarianism', *The American Political Science Review*, 84(1), pp. 3-19.

Regulation of Investigatory Powers Act (2000). Available at: <https://www.legislation.gov.uk/ukpga/2000/23/contents> (Accessed: 2022).

Repko, A. F., Szostak, R. and Buchberger, M. P. (2014) *Introduction to Interdisciplinary Studies*. Los Angeles: SAGE.

Riebe, T. and Reuter, C. (2019) 'Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment', in Reuter, C. (ed.) *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden: Springer Fachmedien Wiesbaden, pp. 165-183.

Riecke, L. (2023) 'Unmasking the Term 'Dual Use' in EU Spyware Export Control', *European Journal of International Law*, 34(3), pp. 697-719.

The Right to Information Act (2005). Available at: https://cic.gov.in/sites/default/files/RTI-Act_English.pdf (Accessed: 2023).

Roberts, A. (2012) 'WikiLeaks: the Illusion of Transparency', *International Review of Administrative Sciences*, 78(1), pp. 116-133.

Robson, C. and McCartan, K. (2016) *Real World Research: A Resource for Users of Social Research Methods in Applied Settings*. 4th edn. Chichester, West Sussex, United Kingdom: John Wiley & Sons.

Roth, Y. and Pickels, N. (2020) *Bot or Not? The Facts About Platform Manipulation on Twitter*. Available at: https://blog.twitter.com/en_us/topics/company/2020/bot-or-not (Accessed: 5 July 2023).

RSF_en (2016) *Iran creates 'Halal Internet' to Control Online Information*. Available at: <https://rsf.org/en/iran-creates-halal-internet-control-online-information> (Accessed: 17 October 2023).

Rudman, R. and Bruwer, R. (2016) 'Defining Web 3.0: Opportunities and Challenges', *Electronic Library*, 34(1), pp. 132-154.

S., R. (2021) 'India's Farmers Have Won - But This Doesn't Mean Modi is Softening', *The Guardian*, 23 November 2021. Available at: <https://www.theguardian.com/commentisfree/2021/nov/23/india-farmers-modi-climbdown-dissent> (Accessed: 29 February 2024).

Sahu, S. (2023) *Unfolding Feminism in India: Women, Power and Politics*. India: Routledge.

Sandelowski, M. (2000) 'Combining Qualitative and Quantitative Sampling, Data Collection, and Analysis Techniques in Mixed-Method Studies', *Research in Nursing & Health*, 23(3), pp. 246-255.

Schauer, F. (2005) 'The Social Construction of the Concept of Law: A Reply to Julie Dickson', *Oxford journal of legal studies*, 25(3), pp. 493-501.

Schmitter, P. C. and Karl, T. L. (1991) 'What Democracy Is. . . and Is Not', *Journal of Democracy*, 2(3), pp. 75-88.

Schmotz, A. (2019) 'Hybrid Regimes', in Merkel, W., Kollmorgen, R. and Wagener, H.-J. (eds.) *The Handbook of Political, Social, and Economic Transformation*. Oxford: Oxford University Press, pp. 521-525.

Scopus (2023a) 'Analyze Search Results: 'Digital AND Authoritarianism' 1980-2023. Available at: <https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=1d14919005f551caaecfcee63e591426&sot=a&sdt=a&sl=39&s=TITLE-ABS-KEY%28digital+authoritarianism%29&origin=resultslst&count=10&analyzeResults=Analyze+results> (First Accessed: 07 October 2023; Re-accessed: 10 February 2025).

Scopus (2023b) 'Analyze Search Results: 'Digital AND Democracy' 1985-2023. Available at: <https://www.scopus.com/term/analyzer.uri?sort=plf->

[f&src=s&sid=1aece5ca3beaa5ba840064870cd71cf3&sot=a&sdt=a&sl=32&s=TITLE-ABS-KEY%28digital+democracy%29&origin=resultslist&count=10&analyzeResults=Analyze+results](https://www.researchgate.net/publication/33840064870cd71cf3&sot=a&sdt=a&sl=32&s=TITLE-ABS-KEY%28digital+democracy%29&origin=resultslist&count=10&analyzeResults=Analyze+results) (First Accessed: 18 October 2023; Re-accessed: 10 February 2025).

Seal, A. (2015) 'Thematic Analysis', in Gilbert, G. N. (ed.) *Researching Social Life*. 4th edn. London: SAGE Publications, pp. 443-460.

Shahbaz, A. (2018) *The Rise of Digital Authoritarianism*. Available at: <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism> (Accessed: 1 August 2022).

Shahbaz, A. and Funk, A. (2019) *Freedom on the Net 2019: The Crisis of Social Media*. Freedom House. Available at: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf (Accessed: 21 November 2024).

Share Checklist (n.d.). Available at: <https://sharechecklist.gov.uk> (Accessed: 14 July 2023).

Siddique, H. (2019) 'British Indians Warn Hindu Nationalist Party not to Meddle in UK Elections', *The Guardian*, 11 November 2019. Available at: <https://www.theguardian.com/politics/2019/nov/11/british-indians-warn-hindu-party-not-to-meddle-in-uk-elections> (Accessed: 27 June 2023).

Simon, J., Bass, T., Boelman, V. and Mulgan, G. (2017) *Digital Democracy: The Tools Transforming Political Engagement*. Available at: https://media.nesta.org.uk/documents/digital_democracy.pdf (Accessed: 25 September 2023).

Simons, H. (2009) *Case Study Research in Practice*. London, United Kingdom: SAGE Publications.

Singh, K. D. and Conger, K. (2022) 'Twitter, Challenging Orders to Remove Content, Sues India's Government', *The New York Times*, 8 July 2022. Available at: <https://www.nytimes.com/2022/07/05/business/twitter-india-lawsuit.html> (Accessed: 19 August 2022).

Soni, K. (n.d.) 'Separation of Powers in India'. Available at: <https://www.legalserviceindia.com/legal/article-6034-separation-of-powers-in-india.html> (Accessed: 2023).

Sørensen, J. K., Van den Bulck, H. and Kosta, S. (2020) 'Stop Spreading The Data: PSM, Trust, and Third-Party Services', *Journal of Information Policy*, 10, pp. 474-513.

Stake, R. (1995) *The Art of Case Study Research*. SAGE Publications.

Statcounter (2024a) 'Social Media Stats India' *January 2020- September 2024*. Available at: <https://gs.statcounter.com/social-media-stats/all/india/#monthly-201901-201912-bar> (Accessed: 24 October 2024).

Statcounter (2024b) 'Social Media Stats United Kingdom' *January 2020- September 2024*. Available at: <https://gs.statcounter.com/social-media-stats/all/united-kingdom/#monthly-201901-201912-bar> (Accessed: 24 October 2024).

Stonewall (n.d.) *Our Impact*. Available at: <https://www.stonewall.org.uk/about-us/our-impact> (Accessed: 5 December 2024).

Stubbs, A. (2023) 'Digital Participatory Democracy: A Normative Framework for the Democratic Governance of the Digital Commons', *Journal of Social Philosophy*, 54(3), pp. 385-403.

Svolik, M. W. (2012) *The Politics of Authoritarian Rule*. Cambridge: Cambridge University Press.

Szostak, R. (2015) 'Interdisciplinary and Transdisciplinary Multimethod and Mixed Methods Research', in Hesse-Biber, S. N. and Johnson, R. B. (eds.) *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*. Oxford University Press, pp. 128-143.

Telecommunications Act (2023). Available at: <https://egazette.gov.in/WriteReadData/2023/250880.pdf> (Accessed: 2024).

The Temporary Suspension of Telecom Services (2017). Available at: <https://thc.nic.in/Central%20Governmental%20Rules/Temporary%20Suspension%20Of%20Telecom%20Services%20Rules,%202017.pdf> (Accessed: 12 October 2025).

Terrorism Act (2006). Available at: <https://www.legislation.gov.uk/ukpga/2006/11/contents> (Accessed: 2022).

The Wire Staff (2022) 'Whistleblower Says Indian Government 'Agent' Was Placed in Twitter to Gauge Company's Plans', *The Wire*, 13 September 2023. Available

at: <https://www.wired.com/story/has-twitters-whistleblower-tanked-elon-musks-takeover/> (Accessed: 2023).

TNM Staff (2021) 'Alt News co-founder Mohammed Zubair Receives Twitter Notice for Tweet from March', *The News Minute*, 11 June 2021. Available at: <https://www.thenewsminute.com/article/alt-news-co-founder-mohammed-zubair-receives-twitter-notice-tweet-march-150524> (Accessed: 8 April 2023).

Tolbert, C. J. and McNeal, R. S. (2003) 'Unraveling the Effects of the Internet on Political Participation?', *Political Research Quarterly*, 56(2), pp. 175-185.

Torfin, J., Andersen, L. B., Greve, C. and Klausen, K. K. (2020) 'Digital Era Governance', in *Public governance paradigms: competing and co-existing*. Northampton: Edward Elgar Publishing.

Tudor, M. (2023) 'Why India's Democracy is Dying', *Journal of Democracy*, 34(3), pp. 121-132.

Uberoi, E. (2023a) *Ethnic Diversity in Politics and Public Life*. Available at: <https://commonslibrary.parliament.uk/research-briefings/sn01156/> (Accessed: 31 January 2024).

Uberoi, E. (2023b) *Turnout at Elections*. Available at: <https://researchbriefings.files.parliament.uk/documents/CBP-8060/CBP-8060.pdf> (Accessed: 30 January 2024).

UK-Facebook (n.d.-a) *Content Restrictions Based on Local Law*. Available at: <https://transparency.fb.com/data/content-restrictions/country/GB/> (Accessed: 2 April 2022).

UK-Facebook (n.d.-b) *Government Request for User Data - UK*. Available at: <https://transparency.fb.com/data/government-data-requests/country/GB/> (Accessed: 2 April 2022).

UK-FiW (2020) *United Kingdom - Freedom in the World 2020*. Freedom House. Available at: <https://freedomhouse.org/country/united-kingdom/freedom-world/2020> (Accessed: 2021).

UK-FiW (2021) *United Kingdom - Freedom in the World 2021*. Freedom House. Available at: <https://freedomhouse.org/country/united-kingdom/freedom-world/2021> (Accessed: 2021).

UK-FiW (2022) *United Kingdom - Freedom in the World 2022*. Freedom House. Available at: <https://freedomhouse.org/country/united-kingdom/freedom-world/2022> (Accessed:2022).

UK-FoN (2019) *United Kingdom - Freedom on the Net 2019*. Freedom House. Available at: <https://freedomhouse.org/country/united-kingdom/freedom-net/2019> (Accessed: 2021).

UK-FoN (2020) *United Kingdom - Freedom on the Net 2020*. Freedom House. Available at: <https://freedomhouse.org/country/united-kingdom/freedom-net/2020> (Accessed: 2021).

UK-FoN (2021) *United Kingdom - Freedom on the Net 2021*. Freedom House. Available at: <https://freedomhouse.org/country/united-kingdom/freedom-net/2021> (Accessed: 2021).

UK-Twitter (n.d.) *Government Removal Request*. Available at: <https://transparency.twitter.com/en/reports/countries/uk.html> (Accessed: 2 April 2022).

UK-Twitter-Web Archive (2022) *Government Information Requests*. Available at: <https://web.archive.org/web/20220528074815/https://transparency.twitter.com/en/reports/countries/uk.html> (Accessed: 9 November 2024).

UKRI (n.d.) *Who ESRC is*. Available at: <https://www.ukri.org/who-we-are/esrc/who-we-are/> (Accessed: 2024).

United Nations Information Service (n.d.) *The UN in General*. Available at: <https://unis.unvienna.org/unis/en/topics/the-un-in-general.html#:~:text=The%20UN%20has%20four%20main%20purposes%3A&text=To%20help%20nations%20work%20together,nations%20to%20achieve%20these%20goals> (Accessed: 10 October 2024).

Universal Declaration of Human Rights (1948) *United Nations Human Rights: Office of the High Commissioner*. Available at: <https://www.ohchr.org/en/human-rights/universal-declaration/translations/english> (Accessed: 2020).

United Nations (n.d.) *About Us*. Available at: <https://www.un.org/en/about-us> (Accessed: 8 December 2024).

Vaidhyanathan, S. (2018) 'The Incomplete Political Economy of Social Media', in J. Burgess, A. Marwick, & T. Poell (Eds.), *The Sage Handbook of Social Media*, pp. 213-229.

van Dijck, J. (2014) 'Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology', *Surveillance & Society*, 12 (2), pp. 197-208.

van Dijk, J. and Hacker, K. L. (2000) *Digital Democracy: Issues of Theory and Practice*. London;Thousand Oaks, California: SAGE.

van Dijck, J. and Poell, T. (2013) 'Understanding Social Media Logic', *Media and Communication (Lisboa)*, 1(1), p. 2.

Vardy, E. (2017) 'Call for Tech Giants to Face Taxes Over Extremist Content', *BBC*, 31 December 2017. Available at: <https://www.bbc.co.uk/news/uk-42526271> (Accessed: 20 August 2022).

Verniers, G. and Ammassari, S. (2019) 'Lok Sabha Election Results 2019: At 14.6%, Lok Sabha to Have Most Women Ever', *Hindustan Times*, 25 May 2019. Available at: <https://www.hindustantimes.com/lok-sabha-elections/lok-sabha-election-results-2019-at-14-6-lok-sabha-to-have-most-women-ever/story-5BCCTbyER96BxdMV22PKPN.html> (Accessed: 4 December 2024).

Walsham, G. (1993) *Interpreting Information Systems in Organizations*. Chichester: John Wiley & Sons.

Warren, M. (2018) 'Trust and Democracy', in Uslaner, E. M. (ed.) *The Oxford Handbook of Social and Political Trust*. Oxford: Oxford University Press, pp. 75-94.

Weber, V. (2017) 'Why China's Internet Censorship Model Will Prevail Over Russia's'. Available at: <https://www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias> (Accessed: 13 October 2023).

Wessels, B. (2018) *Communicative Civic-ness: Social Media and Political Culture*. Abingdon, Oxon: Routledge.

Whittaker, F. (2018) 'What Is WikiLeaks? Everything You Need to Know', *NBC News*, 30 April 2018. Available at: <https://www.nbcnews.com/storyline/smart-facts/what-wikileaks-everything-you-need-know-n869556> (Accessed: 24 October 2023).

Wikileaks (n.d.) *WikiLeaks:Strategy*. Available at: <https://www.wikileaks.org/wiki/WikiLeaks:Strategy> (Accessed: 24 October 2023).

Woodhouse, J. (2023) *Online Safety Bill: Progress of the Bill*. Available at: <https://researchbriefings.files.parliament.uk/documents/CBP-9579/CBP-9579.pdf> (Accessed: 2023).

Woolley, S. C., and Howard, P. N. (2018) 'Introduction: Computational Propaganda Worldwide', in Woolley, S. C., and Howard, P. N. (eds.) *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. New York, NY: Oxford University Press, pp. 3-18.

World Bank (1992) *Governance and Development*. Available at: <https://documents1.worldbank.org/curated/en/604951468739447676/pdf/Governance-and-development.pdf> (Accessed: 28 November 2024).

World Bank (n.d.) 'Individuals Using the Internet (% of population)- United Kingdom' 1990-2021. Available at: <https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2021&locations=GB&start=2019&view=chart> (Accessed: 5 December 2024)

Worldometer (n.d.) 'World Population by Year' -5000 to 2024. Available at: <https://www.worldometers.info/world-population/world-population-by-year/> (Accessed: 2024)

Wright, N. (2019) 'Artificial Intelligence and Domestic Political Regimes: Digital Authoritarian, Digital Hybrid, and Digital Democracy', in *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press, pp. 21-34.

X (n.d.) *Removal Requests*. Available at: <https://transparency.x.com/en/reports/removal-requests.html#2021-jul-dec> (Accessed: 30 April 2024).

Xu, X. (2020) 'To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance: Authoritarian Control In the Age of Digital Surveillance', *American Journal of Political Science*, 65(2), pp. 309-325.

Yayboke, E. and Brannen, S. (2020) *Promote and Build: A Strategic Approach to Digital Authoritarianism*. Center for Strategic & International Studies. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201015_Yayboke_Brannen_PromoteAndBuild_Brief.pdf (Accessed: 9 October 2023).

Young, J. (2023) 'Reflections on Democracy', in Johnson, D. (ed.) *Rethinking Democracy and Governance: Perspectives from the Caribbean*. pp. 21-41.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.